Integrated digital forensic process model

M.D. Kohn [a,*], M.M. Eloff [b,2], J.H.P. Eloff [a,c,1,3]

[a] Department of Computer Science, University of Pretoria, Lynnwood Road, Pretoria 0001, South Africa [b] Institute for Corporate Citizenship, Unisa, PO Box 392, Pretoria 0003, South Africa
[c] SAP New Business and Technology (Mobile Empowerment) Africa, Suite 173, Private Bag X 25, Lynnwood Ridge 0040, South Africa

ABSTRACT

Digital forensics is an established research and application field. Various process models exist describing the steps and processes to follow during digital forensic investigations. During such investigations, it is not only the digital evidence itself that needs to prevail in a court of law; the process followed and terminology used should also be rigorous and generally accepted within the digital forensic community. Different investigators have been refining their own investigative methods, resulting in a variety of digital forensic process models. This paper proposes a standardized Digital Forensic Process Model to aid investigators in following a uniform approach in digital forensic investigations.

Keywords:
Digital forensics
Computer forensics
Digital forensic investigations
Process models
Digital forensic process

1. Introduction

Digital forensics, also known as computer forensics, first presented itself in the 1970s (Pollitt, 2010). During the first investigation, financial fraud proved to be the root cause on the suspect computer. Over the past years digital forensics has become increasingly important in cases where electronic de-vices are used in the perpetration of a crime. Garfinkel (2010) provides a recent historic overview of digital forensic de-velopments. The initial focus of digital forensic investigations was on crimes committed by using computers, but the field has expanded to include different devices where digitally stored information can be manipulated and used for various other criminal related activities.

Digital forensic investigations are common practice in law enforcement and commerce. Rapidly developing technology has resulted in various methods used by investigators to establish the root cause of an incident. This has in turn resulted in a number of digital forensic investigation approaches being proposed, developed and refined. Garfinkel (2010) and Beebe (2009) stated that the lack in digital forensic standardization and process, non-standard computing devices, the problem of scalability are but some of the challenges which result in limited prosecution.

The aim of this paper is firstly to investigate some of the most prominent process models used in digital forensic investigations and secondly, after a comparative analysis of these process models, to propose an Integrated Digital Forensic Process Model or IDFPM that will help overcome some of the problems of the current investigation approaches. The proposed IDFPM consists of the prominent processes as extracted from the process models examined. The proposed

[*] *Corresponding author*. Johannesburg Society of Advocates, 81 Maude Street, Sandton, Johannesburg, Gauteng 2146, South Africa. Tel.: +27 83 457 7112.

E-mail addresses: mkohn@cs.up.ac.za (M.D. Kohn), eloffmm@unisa.ac.za (M.M. Eloff), jan.eloff@sap.com (J.H.P. Eloff).

[1] Tel.: +27 83 457 7112. [2] Tel.: +27 12 433 4604.

3Tel.: þ27 12 999 9100.

IDFPM is a contribution towards a standardized DFPM regarding the processes and terminology used.

The remainder of the paper is structured as follows: the background section discusses some of the definitions of digital forensics in order to derive at working definitions for both digital forensics and digital forensic investigations. Section 3 discusses a number of existing process models within the current literature, while Section 4 introduces the Integrated Digital Forensic Process Model. The paper is concluded in Section 5.

2. Background

The main purpose of the background section is to define digital forensics, a digital forensic investigation, as well as the goal of such an investigation as used in this paper.

2.1. *Digital forensics*

Digital forensics is often defined from the limited perspective of the person involved in an investigation (Ioeng, 2006). This section lists and discusses some of the definitions generally accepted within the literature. Common elements are extracted from these existing definitions to formulate an inclusive definition for digital forensics as used in this paper.

Computer forensics, digital forensics and media analysis, terms used in the field of digital forensics (Carrier, 2005), are found in the literature to describe this sub-branch of forensic sciences (Noblitt and Pollitt, 2000). The term *digital forensics* will be used in this paper.

Palmer (2001) defined *digital forensics* as "the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purposes of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations". This definition is generally accepted to be an all-inclusive definition.

Willassen and Mjølsnes (2005) defined *digital forensics* as "the practice of scientifically derived and proven technical methods and tools towards the after-the-fact digital information derived from digital sources for the purpose of facilitating or furthering the reconstruction of events as forensic evidence".

The main difference between these two definitions is that Willassen and Mjølsnes (2005) removed the criminal element, which broadens the scope of application to include digital forensics in various types of investigations, such as commercial investigations.

Pollitt (2001) states that digital forensics is not a single process but a group of tasks, steps or sub-processes followed during an investigation. It is for this reason that a digital forensic process must be flexible to accommodate various technologies. A static process will limit future developments in the digital forensics field. Robbins (2012) defines computer fo-rensics as "simply the application of computer investigation and analysis techniques in the interests of determining po-tential legal evidence" and does not prescribe the process as methodically as Palmer, but nevertheless includes a number of fixed steps in his explanation. However, formulating a fixed process list in a definition of digital forensics should be avoided.

Reconstruction is listed as an element to help in finding a root cause or simulating the events leading to an investigation. In digital forensics, one investigator should reach the same conclusion as another, even when using different tools (von Solms et al., 2006). Unauthorized actions or actions shown to be disruptive to planned operations must be known or identifiable, prior and during a digital forensic investigation. This knowledge will aid process development and certainty in producing the evidence.

Considering the definitions by Palmer and Willassen and Mjølsnes, as well as other definitions in the literature, digital forensics is, for the purposes of this paper, defined as "a specific, predefined and accepted process applied to data stored digitally or digital media using scientific proven and derived methods, based on a solid legal foundation, to extract after-the-fact digital evidence with the goal of deriving the set of events or actions indicating a possible root cause, where reconstruction of possible events can be used to validate the scientifically derived conclusions".

2.2. *Digital forensic investigation*

A *digital forensic investigation* or DFI is the process to determine and relate extracted information and digital evidence to establish factual information for judicial review (Ioeng, 2006). Ioeng (2006) and Cohen (2010) emphasize the need to establish factual information as the outcome of such investigation.

Carrier (2005) proposes the use of the term DFI rather than digital forensics, and reasons that forensic science addresses a limited hypothesis. In a digital forensic investigation, DNA can be used to determine the relation between the suspect and the device at the physical crime scene (Casey, 2007). In this instance, forensic science aids digital forensic science to determine a solution in the greater DFI, namely to prove whether the suspect was at the crime scene. Non-digital evidence can help an investigator in a DFI to directly establish the presence of the suspect at the scene of the incident. A DFI is therefore the process of identifying potential evidence, digital or non-digital, *and* identifying the unique source of the po-tential evidence (Carrier, 2005). Cohen (2009) includes attribution as a process in his DFPM where the resulting digital evidence is linked to a specific person.

A *forensic investigation* of digital evidence is employed as a post-event response to an incident (Rowlingson, 2004). A *DFI* is therefore a special 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. Since digital evidence is contained on some electronic media and cannot be viewed with the naked eye, some tool will be used to examine the state of this digital data. Tools used to observe the state of digital data constitute an indirect data observation. Tools used in DFIs include, but are not limited to, Encase (Guidance Software, 2011) and FTK (Access Data, 2011). The weight attributed to the evidential value is based on the extent to which the tool is trusted (Wojcik et al., 2006; Patel and Ciardhua´ in, 2000). The confidence in DFIs is based on the level of trust in the hardware and software used to collect and analyse the data (Carrier and Spafford, 2003). Trust in the ability and experience of the investigator also contributes to the level of confidence in a digital forensic investigation when expert testimony is presented in court.

DFI, for the purpose of this paper, is therefore defined, as a special type of investigation where the scientific procedures followed and techniques used will allow the results – digital evidence – to be admissible in a court of law or a disciplinary forum in a corporate organization.

Any digital forensic investigation conducted has a very specific purpose or outcome, namely admissible digital forensic evidence that will aid judicial review. An investigation is generally initiated with the aim to establish some facts about an event that has taken place. The primary goal in establishing a possible root cause is to ensure that the investigation is conducted in a manner that will withstand legal scrutiny when the matter is serious enough to warrant it. However, any investigation should be conducted methodically to ensure that the conduct of the investigator is of such a nature that the validity of the evidence produced cannot be questioned. It should be noted that various types of DFIs exist. These include live forensics, proactive forensics and network forensics (Beebe and Clark, 2004; Rogers et al., 2006; Mylonas et al., 2012). Live forensics refers to the collection of digital evidence from running systems, which include contextual information that is no longer available when data is collected after the incident (Adelstein, 2006). Proactive forensics means taking steps to anticipate the need to locate the unauthorized actions for examination. With proactive forensics the ability to collect credible digital evidence will be maximized while the cost of the investigation will be minimized (Mylonas et al., 2012). Beebe and Clark (2004) suggest a second-tier phase to the DFI, which specifically anticipates steps followed in specific incident investigations. Types of incidents include drug activity, financial crimes and child pornography.

Rogers et al. (2006) propose a digital evidence triage to aid the investigator. The evidence triage consists of the user usage profile, Internet usage and chronological timeline activity. The specific user evidence is found in home directories, the registry and file properties. Depending on the type of investigation conducted the evidence triage will guide an investigator to possible evidence, if other traces have possibly been removed.

The fundamental point of departure for any investigation is to answer basic questions about the evidence. In addition to knowing what happened, there is a need to know who is responsible (Kruse and Heiser, 2002). Zachman (2003) developed a framework adapted by Ieong (2006) and Beebe and Clark (2004) proposing that every investigator should ask the following six key questions during an investigation (Ieong, 2006; Beebe and Clark, 2004): what, why, how, who, where and when. *What* is determined by the data attributes or metadata, *why* refers to the motivation, *how* is the procedure followed to initiate the incident or isolate the necessary evidence, *who* are the people involved, *where* refers to the location and *when* refers to time.

The next section deals extensively with the question of *how* evidence was found in an investigation. The *how* question is addressed by the steps of the process followed, and these steps have to be defined. Various authors have described these steps in a Digital Forensic Process Model or DFPM.

3. Selected existing digital forensic process models (DFPMs)

The primary objective of a DFPM is to aid the investigator to explain *how* specific digital evidence is found on a device. A number of DFPMs exist in the current literature. The DFPM processes and terminology up to date have not been formally standardized. Some digital forensic investigation process descriptions in the literature include high level phased descriptions such as preparing for an electronic investigation and validating electronic evidence (Wolfe, 2003), reconstruction and hypothesis testing (Carrier and Spafford, 2004b). Detailed process step descriptions are found in DFPMs proposed by Ciardhua´ in (2004), Carrier and Spafford (2003). Authors use different ways to present their DFPMs, including descriptions, process models and state diagrams. Both the high level and detailed approaches are characterized by non-standard pro-cess descriptions and conflicting terminology. This section will discuss a limited number of existing DFPMs found in the cur-rent literature. The section will conclude with a table which identify the common processes used in the DFPMs.

The paper is limited to a discussion of the following DFPMs: Lee et al. (2001), Casey (2004), Carrier and Spafford (2004a), Baryamureeba and Tushabe (2004), Ciardhua´ in (2004) and Cohen (2009). Numerous other DFPMs were examined in the initial research but the discussion in this paper has been limited to the listed DFPMs as they are the DFPMs that have the most detailed sub-processes listing and are contained in those not listed here. All the process descriptions included in the DFPMs are discussed.

3.1. *Methodology*

To uniformly represent the DFPMs as discussed in this paper, a number of visual and formal representations were considered. These include, but are not limited to, UML Activity, Use Case Diagrams (Kohn et al., 2008) and Finite State Machines (Carrier and Spafford, 2006; Cohen, 2009). For the purposes of this paper the ordering of the events or processes are considered critical. Sequential logic as formulated by Moore and Mealy (Nair, 2006) is used in the remainder of the paper.

Sequential logic is proposed to represent the DFPMs because the circuit outcome is dependent on the input and the current internal state. For the circuit to evaluate true, all the conditions of the previous states must be true. The circuit will fail if the current state is not positively completed (Nair, 2006). This will allow an investigator to revisit previous steps in the process, but he/she will not be able to continue if a step is not complete or fails.

The sequential logic notation is however adapted to uniformly represent each of the DFPMs, where the list values have been directly replaced with the process steps. The adapted sequential notation is illustrated here as:

$$\text{DFPM} = \{start \Rightarrow next \Rightarrow then \ldots end\}$$

In certain instances where sub-processes are indicated, these will be illustrated when introducing the DFPMs. Parallel processes are indicated by $||$. $\Leftrightarrow$ is used where a previous process can be repeated after executing the current process.

Each DFPM is shown using the adapted sequential logic notation. This is done to identify similarities and differences within the sequence of tasks when conducting a digital forensic investigation. Terminology used in the DFPMs is listed and briefly defined where new terms are introduced. Brief comments, if any, conclude the discussion on each DFPM.

3.2. *Lee*

Henry Lee formulated a Scientific Crime Scene Investigation model (Lee et al., 2001) used in forensic science investigations. Lee's model was not developed within the digital forensics field, but has had a considerable influence on DFPMs nonetheless. This DFPM is represented as:

$$\text{Lee} = \{\mathit{Recognize} \Rightarrow \mathit{Identify} \Rightarrow \mathit{Individualize} \Rightarrow \mathit{Reconstruct}\}$$

where

$$\begin{aligned}&\mathit{Recognize} = \{\mathit{Document} \Rightarrow \mathit{Collect\ and\ Preserve}\}\\&\mathit{Identify} = \{\mathit{Classify} \Rightarrow \mathit{Compare}\}\\&\mathit{Individualize} = \{\mathit{Evaluate} \Rightarrow \mathit{Interpret}\}\\&\mathit{Reconstruct} = \{\mathit{Reconstruct} \Rightarrow \mathit{Report\ and\ Present}\}\end{aligned}$$

The terminology used is described as follows:

Recognition is where items or patterns are seen to be potential evidence. The investigator must know what to look for and where to find it. This sub-process has two activities, namely *documentation* and *collection and preservation*. Documenting evidence during an investigation is when any action by any person is recorded. Beebe and Clark (2004) suggest that every phase of an investigation must be thoroughly documented throughout the entire investigation process, especially during preservation because this will have an influence on the chain of evidence which will need to be explained at the forum where the evidence is presented. Collection is where the evidence is collected from the crime scene, before being *bagged and tagged*. Digital evidence must be preserved once safely contained. Collection and preservation is seen as a single process step in this DFPM.

Identification of the various types of evidence follows after recognition. Evidence is classified, usually into categories such as physical, biological, chemical and other standard types and compared (Ciardhua´ in, 2004).

Individualization is where evidence is linked to a particular individual or event. The evidence is then evaluated and interpreted. *Reconstruction* is where evidence objects and events are linked so as to account for a possible sequence of events. During reconstruction, possible event sequences are reported and presented (Lee et al., 2001). Reporting and presenting is considered to be a single process step in this DFPM.

Ciardhua´ in (2004) criticizes Lee's model because it deals specifically with the physical crime scene investigation and not with the entire digital forensic investigative. Ciardhua´ in's (2004) criticism does not include a solution, but advocates that the investigation must be systematic and methodical. Though Lee's model focuses on physical evidence, it can be adapted to include evidence found in a digital crime scene investigation. The physical evidence, including any digital media, is usually processed for trace evidences such as blood and DNA.

3.3. *Casey*

In 2000 Casey proposed a DFPM for processing and examining digital evidence. This DFPM can be applied to various investigations, including standalone computer systems and networked environments (Ciardhua´ in, 2004). In 2004 Casey revised his DFPM to include a number of additional processes (Casey, 2004). The 2000 Casey DFPM is listed as:

$$\begin{aligned}\text{Casey 2000} = \{&\mathit{Recognition} \Rightarrow \mathit{Preservation} \Rightarrow \mathit{Classification}\\&\Rightarrow \mathit{Reconstruction}\}\end{aligned}$$

where

$$\begin{aligned}&\mathit{Preservation} = \{\mathit{Collect} \Rightarrow \mathit{Document}\}\\&\mathit{Classification} = \{\mathit{Compare} \Rightarrow \mathit{Individualize}\}\end{aligned}$$

The DFPM by Casey (2000) is similar to the model proposed by Lee. Casey's model is aimed at processing and examining digital evidence (Baryamureeba and Tushabe, 2004); however his analysis differs substantially from the physical analysis of non-digital evidence types in the model by Lee. The first and last processes, namely recognition and reporting, are identical in both these DFPMs. The 2004 Casey model is significantly extended and is given as:

$$\begin{aligned}\text{Casey 2004} = \{&\mathit{Incident\ Recognition} \Rightarrow \mathit{Assessment} \Rightarrow \mathit{Identification}\\&\mathit{and\ Seizure} \Rightarrow \mathit{Preservation} \Rightarrow \mathit{Recovery} \Rightarrow \mathit{Harvesting}\\&\Rightarrow \mathit{Reduction} \Rightarrow \mathit{Classification} \Rightarrow \mathit{Analysis} \Rightarrow \mathit{Reporting}\}\end{aligned}$$

where

$$\begin{aligned}&\mathit{Preservation} = \{\mathit{Collect} \Rightarrow \mathit{Document}\}\\&\mathit{Classification} = \{\mathit{Organize} \Rightarrow \mathit{Compare} \Rightarrow \mathit{Individualize}\}\end{aligned}$$

The terminology used by Casey (2004) is described as follows:

Recognition is where the investigator looks similar patterns that might have presented itself in the past. This is a form of investigator experience based on previous investigations and could include a database of previously solved investigations.

Preservation consists of two sub-processes namely *collect* and *document*. During preservation the digital evidence process should firstly ensure quality and continued availability; and secondly maintain the integrity of the evidence during the entire investigation process.

During *classification*, evidence objects are *compared* and *individualized*. *Individualization* is where evidence is attributed to an origin or creator (Cohen, 2009).

During *reconstruction*, the sequence of the crime is traced by reconstructing the possible sequence of events that most accurately reflects the events as they could have occurred during the actual crime or incident. Reconstruction is generally required to prove *how* a certain result is achieved for various purposes.

3.4. *Carrier and Spafford*

Carrier and Spafford's DFPM is named the Integrated Digital Investigation Process (IDIP) which has five sub-processes and seventeen activities in total (Carrier and Spafford, 2004a). This model has a linear sequential logic representation which distinguishes it from the DFPMs by Lee and Casey in the previous sections.

The Carrier and Spafford DFPM is given as:

$$\begin{aligned}\text{Carrier and Spafford} = \{&\textit{Readiness} \Rightarrow \textit{Deployment} \Rightarrow \textit{Physical}\\ &\textit{Investigation} \| \textit{Digital Investigation}\\ &\Rightarrow \textit{Review}\}\end{aligned}$$

where the digital and physical investigations occur simultaneously, and

$$\begin{aligned}\textit{Readiness} &= \{\textit{Operational Readiness} \Rightarrow \textit{Infrastructure Readiness}\}\\ \textit{Deployment} &= \{\textit{Detection and Notification} \Rightarrow \textit{Confirmation and}\\ &\qquad \textit{Authorization}\}\\ \textit{Physical Investigation} &= \{\textit{Preservation} \Rightarrow \textit{Survey} \Rightarrow \textit{Documentation}\\ &\qquad \Rightarrow \textit{Search and Collection} \Rightarrow \textit{Reconstruction}\\ &\qquad \Rightarrow \textit{Presentation}\}\\ \textit{Digital Investigation} &= \{\textit{Preservation} \Rightarrow \textit{Survey} \Rightarrow \textit{Documentation}\\ &\qquad \Rightarrow \textit{Search and Collection} \Rightarrow \textit{Reconstruction}\\ &\qquad \Rightarrow \textit{Presentation}\}\end{aligned}$$

The terminology used in this DFPM is similar to the definitions in the previous models. During the *review* phase the whole investigation is reviewed and areas of improvement are identified. It is interesting to note that this DFPM includes a physical and digital investigation to be conducted concurrently. For the full discussion see Carrier and Spafford (2004a).

This DFPM includes sub-processes during investigation to accommodate issues such as data protection, acquisition, imaging, extraction, interrogation, ingestion and normalization, analysis and reporting (Baryamureeba and Tushabe, 2004). High-level processes are included for both the physical and logical or digital crime scenes. Baryamureeba and Tushabe (2004) question the practicality of the model. The following situation illustrates the problem: The primary crime scene is where the crime is initiated. The target of the malicious activity is victim's location, the secondary crime scene, which is not part of the physical or digital forensic investigation. The result of the malicious activity is not included in the investigation, which will impact on the possible reconstruction of a sequence of events. This can lead to incomplete findings in the report presented.

Carrier and Spafford's inclusion of the physical crime scene is however a notable contribution. Differentiating between a physical and digital crime scene seems trivial, but this distinction is critical for the practical execution of an investigation.

3.5. *Baryamureeba*

The Enhanced Integrated Digital Investigation Process (EIDIP) DFPM also makes a clear distinction between the physical and digital crime scene investigation processes (Baryamureeba and Tushabe, 2004). This DFPM is an extension of the DFPM proposed by Carrier and Spafford and is given as:

$$\begin{aligned}\text{Baryamureeba} = \{&\textit{Readiness} \Leftrightarrow \textit{Deployment} \Leftrightarrow \textit{Traceback}\\ &\Leftrightarrow \textit{Dynamite} \Leftrightarrow \textit{Review}\}\end{aligned}$$

where

$$\begin{aligned}\textit{Readiness} &= \{\textit{Operational Readiness} \Rightarrow \textit{Infrastructure Readiness}\}\\ \textit{Deployment} &= \{\textit{Detection and Notification} \Rightarrow \textit{Physical Crime Scene}\\ &\qquad \textit{Investigation} \Rightarrow \textit{Digital Crime Scene Investigation}\\ &\qquad \Rightarrow \textit{Confirmation} \Rightarrow \textit{Submission}\}\\ \textit{Traceback} &= \{\textit{Digital Crime Scene Investigation} \Rightarrow \textit{Authorization}\}\\ \textit{Dynamite} &= \{\textit{Physical Crime Scene Investigation} \Rightarrow \textit{Digital Crime}\\ &\qquad \textit{Scene Investigation} \Rightarrow \textit{Reconstruction}\\ &\qquad \Rightarrow \textit{Communication}\}\end{aligned}$$

The terminology used by Baryamureeba and Tushabe (2004) is discussed in the following paragraphs.

Readiness includes the training of personnel and the provision of sufficient resources and infrastructure to deal with the investigation.

Deployment as a process includes mechanisms to detect and confirm incidents, and it consists of five sub-processes. The first is to detect the incident and notify the appropriate authority. Secondly, the physical crime scene is examined to identify potential evidence. Thirdly, the potential digital evidence is subjected to a digital examination of potential evidence. Fourthly, confirmation of the incident is given to obtain legal authorization or approval, which can be in the form of a search warrant. Lastly the evidence is presented to the appropriate forum.

In the *Traceback* phase, the physical crime scene is tracked down to identify devices used in the execution of the crime. Firstly the primary crime scene is reconstructed from evidence collected during deployment. This typically includes finding the host computer within a networked environment and then obtaining authorization to permit further investigation of the acquired evidence.

The digital crime scene is processed in a virtual environment created by hardware and software (Baryamureeba and Tushabe, 2004). The phases listed are preservation, survey, search and collection, and documentation. The preservation phase includes the duplication of digital media. During the survey the investigator identifies and separates potential useful data from the imaged set. Hidden, deleted, manipulated or damaged data files are recovered during the search and collect phase. Documentation involves the extensive documenting of all the evidence found, which in turn is useful in the presentation phase.

The *Dynamite* phase investigates the primary crime scene. It is aimed at collecting and analysing evidence items found at the primary scene so as to find the incident perpetrators. This phase involves four sub-processes. First the physical evidence found at the crime scene is examined, followed by examining the digital crime scene. Thirdly possible events are reconstructed to formulate a possible hypothesis. Fourthly, the final interpretations are communicated in a presentation to the appropriate forum.

Lastly, the investigation is reviewed and areas of improvement are identified.

The Baryamureeba DFPM builds on the work of Carrier and Spafford. Carrier and Spafford propose a waterfall type model in their original paper, which does allow splash back to previous phases. Baryamureeba adapts their process flow enabling the investigator to backtrack to previous phases, which is indicated here with a bi-directional arrow between phases.

The shortcoming in Carrier and Spaffor's DFPM is addressed by including an investigation of the primary and secondary crime scenes. In Baryamureeba's DFPM a new phase is introduced where the primary crime scene is identified in the traceback phase. The primary crime scene is the place where the incident originated and the secondary crime scene is where the attack took place. Reconstruction is done only once in this DFPM when all the necessary evidence has been collected.

3.6. Ciardhuáin

The DFPM proposed by Ciardhua´ in (2004) is probably the most all-inclusive and comprehensive to date. The steps or phases are also called activities. The steps are discussed in depth by Ciardhua´in (2004). Only the terms that have not previously been listed are introduced here. Ciardhua´ in's DFPM is a linear representation and is represented as follows:

$$\begin{aligned}\text{Ciardhuáin} = \{ & \mathit{Become\ aware} \Rightarrow \mathit{Authorize} \Rightarrow \mathit{Plan} \Rightarrow \mathit{Notify} \\ & \Rightarrow \mathit{Search/Identify} \Rightarrow \mathit{Collect} \Rightarrow \mathit{Transport} \Rightarrow \mathit{Store} \\ & \Rightarrow \mathit{Examine} \Rightarrow \mathit{Hypothesize} \Rightarrow \mathit{Present} \Rightarrow \mathit{Prove/Defend} \\ & \Rightarrow \mathit{Disseminate}\}\end{aligned}$$

The processes follow the waterfall model, in other words processes follow one another in sequence. Certain sequences can be repeated if needed. The sequence of examine, hypothe-sis, presentation and prove/defend will often be repeated as the evidence pool grows during the investigation (Ciardhuain, 2004).

Awareness is defined as the phase during which the investigators are made aware that a crime has taken place, i.e. the crime is reported to some authority. An intrusion detection system can also trigger such awareness. Ciardhua´ in (2004) specifically includes this in the DFPM because the method of becoming aware could influence the investigation. The investigation will have to be conducted regardless if the investigator has prior knowledge of the type of incident, or not. The co-operation of various parties can be expected, e.g. in cases such as internal investigations where the parties would like to find the root cause of the incident. Awareness can be internal or external to an organization.

Authorization is where the type of investigation has been identified and now the appropriate authorization may be required to proceed. Authorization is acquired internally and/or externally.

Planning is influenced by information within and outside the organization that will impact on the investigation. Outside factors include legal and other requirements that are not determined by the investigators, while internal factors include organizational policies, procedures and other prior investigative knowledge. The scope can also be backtracked if the full requirements of the investigation are not included in the planned scope. Externally imposed policies, regulations and legislation, external information, information distribution and organizational policies can influence the planning phase.

During *notification* the stakeholders or subject investigated is informed that an investigation is taking place. In cases where the subject investigated must not know that an investigation is taking place, this step is omitted. Other interested parties can also be informed that there is an investigation in progress during this step.

The *search and identification* of evidence is where the location of the potential evidence is identified. In large investigations this may include finding routes of information flows over ISPs. Authorization will probably have to be revisited in cases of multiple jurisdictions.

Collection occurs when the investigator takes physical possession of the evidence to be preserved and analysed. Ciardhua´ in (2004) includes hard disk imaging and seizing of entire computers in this step. The primary focus of the current literature on digital forensics is on the collection of digital evidence. Mistakes and incorrect procedures during this process will render evidence in later stages useless and therefore inadmissible in court. Where a questionable procedure is followed or cannot appropriately be explained during a court hearing, the digital evidence could be ruled inadmissible. Many legal practitioners will focus on the collection procedure followed to find a questionable procedure in an attempt to invalidate the incriminating evidence.

After collection, the evidence is *transported* to a suitable location for forensic examination. It is important that the integrity of the evidence is not affected physically or digitally during transfer. Digital evidence is stored in a safe location before examination. The integrity of the evidence must also be ensured at the storage location.

Examination is the core process of the digital investigation. A large number of techniques have to be used to access, find and extract evidence from the collected media. When large volumes of data need to be investigated, automated techniques may be required to aid the investigator. Ciardhua´ in (2004) specifically mentions that during examination some automated techniques are required to aid the investigator.

The *hypothesis* formulated by the investigator is based on his/her examination of the digital evidence. The hypothesis is the investigator's proposed construction of events or a possible sequence of events leading to the reported violation. The document compiled during the investigation must reflect the findings of the digital forensic investigator. Backtracking during examination is expected as the investigator gains insight into the investigation. The formulated hypothesis may present the investigator with internal and external challenges. An external challenge could for example be the legal relevance of evidence found during an investigation. An internal challenge could be that there is no digital evidence to support the formulated hypothesis.

Presentation is where the hypothesis is presented to people other than the investigators, such as a jury or management. A decision will then be made on the basis of the presented findings.

The *proof* or *defence* is where the digital forensic investigator questions or substantiates his/her original investigation hypothesis. The investigator will have to defend the findings, or prove that the events occurred as explained in the presentation.

Dissemination of the lessons learnt is the final activity, if required. Policies and procedures influencing future investigations have to be integrated with current policies and procedures.

According to Ciardhuain (2004), the reason for proposing this model is the fact that, while other DFPMs focus on processing digital evidence, this model incorporates the whole investigation process. A lack of standardized terminology also seems to be an identified problem that needs a solution. The process only gives guidance on *what* must be done and not *how*. This DFPM does not include specifics such as tools and technology to be used, or the training needed before an investigator is qualified to do an investigation. Best practices, common experiences and the development of standards are identified as important future research topics.

Ciardhua´ in (2004) as well as Carrier and Spafford (2004a) also remark that information flows are not addressed in any of the previous DFPMs discussed. The main problem in this regard is where and how the chain of custody is compiled. Different legal systems, best practices and languages are some difficulties that investigators could encounter.

Awareness, transport, storage and dissemination are considered irrelevant according to a survey conducted by Ciardhua´in (2004). The remainder of the proposed DFPM activities was considered relevant. In contrast to the view expressed by Ciardhua´in that awareness is irrelevant, Perumal (2009) states that awareness should be extended to be a three-step process. The sub-processes proposed by Perumal include the complaint, investigation and prosecution. The Ciardhua´in DFPM only includes the complaint step.

Ciardhua´ in's (2004) later work includes policy development on criminal investigations, auditors, civil litigation, system administrator investigations and judicial inquiries.

3.7. *Cohen*

The DFPM proposed by Cohen (2009) consists of seven listed processes or phases. The focus of this DFPM is the digital forensic examination. The Cohen DFPM is given as:

$$\text{Cohen} = \{\mathit{Identification} \Rightarrow \mathit{Collection} \Rightarrow \mathit{Transportation} \Rightarrow \mathit{Storage} \Rightarrow \mathit{Examination\ and\ Traces} \Rightarrow \mathit{Presentation} \Rightarrow \mathit{Destruction}\}$$

where

$$\mathit{Examination} = \{\mathit{Analysis} \Rightarrow \mathit{Interpretation} \Rightarrow \mathit{Attribution} \Rightarrow \mathit{Reconstruction}\}$$

Analysis is where evidence is understood and characterized relative to the legal issue at hand. Beebe and Clark (2004) propose an iterative sub-process listing as survey, extract and examine during analysis. The sub-processes analysis includes the physical media, media management, file system, application and network hierarchy.

Interpretation takes the analysed results and produce meaningful statements which give meaning to the legal and technical situation. *Attribution* involves drawing conclusions about causes and effects. Existing links are identified and documented. A particular cause will give rise to an effect; conversely, a particular effect may or may not be caused by a certain action or incident.

Reconstruction is the process by which a set of mechanisms, similar to those identified, has caused the effect of the digital evidence produced. Reconstruction is therefore a process where the investigator lists certain assumptions and limitations to most accurately present how evidence came to exist.

The focus of the Cohen DFPM is on the examination of digital evidence. It is interesting to compare the examination sub-process listing given by Casey with that of Cohen. This clearly indicates the need for some standardization of terminology. The issue is constantly mentioned by various authors but never sufficiently addressed.

A comparison of the set of activities included under *ex-amination* by Casey (2004) and Cohen (2009) respectively re-veals the following two sets:

$$\text{Casey} : \mathit{Examination} = \{\mathit{Recovery}, \mathit{Harvesting}, \mathit{Reduction}, \mathit{Classification}\}$$

and

$$\text{Cohen} : \mathit{Examination} = \{\mathit{Analysis}, \mathit{Interpretation}, \mathit{Attribution}, \mathit{Reconstruction}\}.$$

Clearly not a single sub-process within the two identified sets has the same meaning. A possible explanation for this discrepancy is that the interpretations of the terms *examine* and *analyse* has been exchanged by the authors.

3.8. *Summary of DFPMs*

From the discussion of the selected DFPMs, it is clear that each one has a slight different focus. Table 1 is a summary of the DFPMs presented in an effort to compare them. The rows indicate the different phases and processes as identified and discussed. The table columns list the six DFPMs discussed in this section.

The *P* is an indication of the DFPM processes and *S-P* the sub-processes. Although the process ordering is considered important in modelling the IDFPM, the *P* and *S-P* indices, indicating the order, have been excluded in Table 1.

The processes in the table listed in italics are those processes identified in DFPMs but were not discussed in this paper. Policy and procedure documentation should be included as a starting point (Tan, 2001). The digital evidence must be authenticated to confirm the data integrity and authenticity (Casey, 2004). Communication between the various investigators is encouraged to suitably explain the events leading to the incident. These discussions should be debated and tested before drafting the final report. A decision is reached by an independent objective forum after the report has been presented.

The phases identified in Table 1 are based on role players involved in the investigation and the different locations identified in the initial research. The locations include the digital forensic organization, the lab, primary and secondary locations. The presentation location is where the final report will be presented.

4. The integrated DFPM (IDFPM)

This section introduces the IDFPM based on the six DFPMs discussed in the previous paragraphs. The focus of the discussion is providing uniform process terminology as extracted from the discussed IDFPMs.

The terminologies used in the discussed DFPMs often differ, but there are similarities. The DFPM process descriptions are studied to find similar meaning in the terminology so as to effectively reduce the number of required processes. Eliminating processes from the DFPMs that have similar objectives also reduces duplicate processes.

The Integrated Digital Forensic Process Model or IDFPM consists of the following processes: *preparation*, *incident*,

Table 1 – Comparative summary of the DFPM discussed.

Phase	Process	Lee	Casey	Carrier & Spafford	Baryamureeba	Ciardhuáin	Cohen
Preparation	*Policy and Procedure*						
	Infrastructure Readiness			S-P	S-P		
	Operational Readiness			S-P	S-P		
Incident	Detect	P	P	S-P	S-P	P	
	Assess		P				
	Confirm			S-P	S-P		
	Notify			S-P	S-P	P	
	Authorise			S-P	S-P	P	
	Deploy			P	S-P		
	Approach Strategy					P	
	Search					P	
	Recover		P				
	Seize		P				
	Preserve	S-P	P	S-P			
	Transport					P	P
	Store					P	P
Digital Forensic Investigation	Collect	S-P	S-P	S-P		P	P
	Authenticate						
	Examine					P	P
	Harvest		P				
	Reduce		P				
	Identify	P	P			P	P
	Classify	S-P	P				
	Organize		S-P				
	Compare	S-P	S-P				
	Hypothesise					P	
	Analyse		P				S-P
	Attribute	P	S-P				S-P
	Evaluate	S-P					
	Interpret	S-P					S-P
	Reconstruct	P		S-P	S-P		S-P
	Communicate						
	Review			P			
Presentation	Present report		P	S-P	S-P	P	P
	Decide						
	Disseminate					P	P

P = Process.
S-P = Sub-process.

incident response, *physical investigation*, *digital forensic investigation* and *presentation*.

The IDFPM process listing is given as:

$$\mathrm{DFPM} = \{\{\mathit{Preparation} \Rightarrow \mathit{Incident} \Rightarrow \mathit{Incident\ Response} \Rightarrow \mathit{Physical\ Investigation} || \mathit{Digital\ Forensic\ Investigation} \Rightarrow \mathit{Presentation}\} || \mathit{Documentation}\}$$

where

$$\mathit{Preparation} = \{\mathit{Policy/Procedure} \Rightarrow \mathit{Operational\ Readiness} || \mathit{Infrastructure\,Readiness}\}$$
$$\mathit{Incident} = \{\mathit{Detect} \Rightarrow \mathit{Assess} || \mathit{Confirm} \Rightarrow \mathit{Notify} \Rightarrow \mathit{Authorize} \Rightarrow \mathit{Deploy}\}$$
$$\mathit{Incident\,Response} = \{\mathit{Approach\,Strategy} \Rightarrow \mathit{Search} \Rightarrow \{\mathit{Recover} || \{\mathit{Seize} \Rightarrow \mathit{Preserve}\} || \mathit{Preserve}\} \Rightarrow \{\mathit{Transport} \Rightarrow \mathit{Store} \Rightarrow \mathit{Collect}\}\}$$
$$\mathit{DFI} = \mathit{Collect} \Rightarrow \mathit{Authenticate} \Rightarrow \mathit{Examine} \Rightarrow \mathit{Harvest} \Rightarrow \mathit{Reduce} \Rightarrow \mathit{Identify} \Rightarrow \mathit{Classify} \Rightarrow \mathit{Organize} \Rightarrow \mathit{Compare} \Rightarrow \mathit{Hypothesize} \Rightarrow \mathit{Analyze} \Rightarrow \mathit{Attribute} \Rightarrow \mathit{Evaluate} \Rightarrow \mathit{Interpret} \Rightarrow \mathit{Reconstruct} \Rightarrow \mathit{Communicate} \Rightarrow \mathit{Review} \wedge \{\mathit{Reconstruct} \Rightarrow \mathit{Hypothesize}\}$$
$$\mathit{Presentation} = \{\mathit{Report/Present} \Rightarrow \mathit{Decide} \Rightarrow \mathit{Dissemination}\}$$

4.1. *Documentation*

The Documentation process is included in the IDFPM as a continuous process and includes the investigation documents and chain of custody recorded as accurately as possible throughout the entire investigation. The diagrammatic representation on the IDFPM is illustrated in Fig. 1. When developing the policies and procedures in an organization, it is essential to ensure that legal advice is sought to ensure any documentation will be able to withstand legal scrutiny. Any deviation from the policies and procedures developed in preparation should thoroughly be documented to ensure the chain of evidence is maintained.

The primary purpose of the documentation is to serve as an investigation log to the investigator who will ultimately testify, in many instances long after the incident occurred, what procedure and investigative techniques were used to admit the final digital evidence.

Documentation starts during preparation when the organization must compile a policy and procedure document on its approach to digital forensic investigations. After the detection of the first incident, the scene must be fully

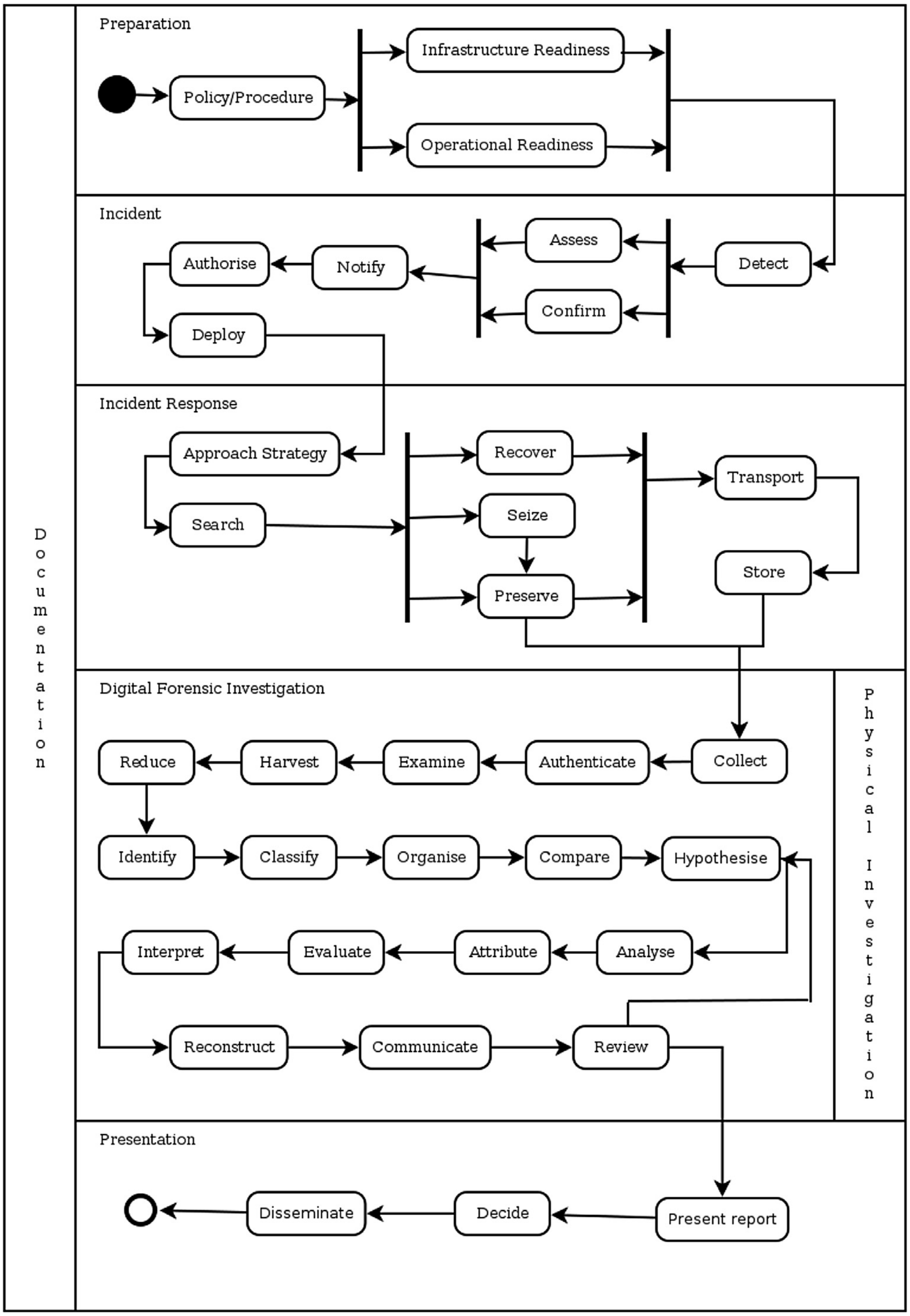

Fig. 1 – The IDFPM illustrated as a process flow diagram.

documented to enable easy physical reconstruction by the investigator during the digital forensic investigation. First responders arriving at the incident are not always equipped to effectively deal with documentation as required by the digital forensic investigation. It is therefore important that they are adequately trained to have a minimum required level of training before deployed to the incident. It is equally important that the first responders record the physical scene as accurately as possible to aid both the physical and digital forensic investigators as the investigation progresses.

The method of documenting is not as important as ensuring that every sub-process is accurately described in documentation for later reference. The documentation should as a minimum include investigator notes to enable other investigators to reach the same conclusion. The investigator must ensure that the chain of custody and chain of evidence are fully and accurately documented.

The documentation will form the basis of the digital evidence ultimately submitted to court. The digital evidence produced is presented in a report document with the findings of the investigator. The report presented includes the methods and techniques used during the investigation, the documented digital evidence presented, the chain of evidence, chain of custody and the expert opinion of the investigator.

4.2. *Preparation*

Preparation is the single most critical process in the IDFPM. This is where the organization enables itself to deal effectively with various types of incidents. Tan (2001) encapsulates this process by stating that forensic readiness has two main objectives, firstly to maximize the collection of credible digital evidence from an incident environment, and secondly to minimize the cost of a forensic incident response.

The focus of forensic readiness is to differentiate between various types of investigations where an operational and infrastructure readiness is already established. Operational and infrastructure readiness is included as a component in the preparation process. In a mobile forensic investigation the same IDFPM is used in forensic readiness, however, on infrastructure level a mobile forensic kit will have to be procured. The kit will improve the organizational operational infrastructure.

The initial policy and procedure documents need to be in place before an organization can successfully initiate digital forensic investigations. The documents should contain a clear description of how the organization will deal with digital evidence for the purposes of an investigation. The objective of the documents is to ensure that a minimum standard of integrity is maintained during investigations when dealing with digital evidence. The organization must be aware of international standards that might be applicable in instances where various disciplines are interested in the findings of the investigation. The documentation should continuously be revised after each investigation to ensure that it is in line with developments in technology.

Operational readiness is determined by factors external and internal to the organization. External factors include, but are not limited to, the legal system, territory legislation, rules of evidence and type of investigations conducted. Internal factors include the training of appropriately qualified personnel (Baryamureeba and Tushabe, 2004). The investigators have to be fully aware of both types of influences within the organization and possible limitations. Any defects may be exploited during presentation of the digital evidence findings.

4.3. *Incident*

An incident may be any action performed to compromise the confidentiality, availability and integrity of an information system. Digital forensics specifically deals with data found on digital media. The incident scope will have to be determined by the type of investigation conducted.

An incident may be detected by an automated incident detection system, or a similar set of event sequences is recognized by an investigator, based on possible previous experience. A comparative database should be developed to include possible new unknown types of incidents, how they were detected, what the findings were and possible guidelines in expediting the investigation. An incident can also be brought to the attention of the appropriate authorities by some external reporting method.

An investigator, who should determine an appropriate approach strategy, must assess the incident anomaly detected. The detected incident should be confirmed by some other source before action is taken towards an incident response. Once an incident is confirmed, the investigators should be notified to initiate an incident response.

Before any incident can be investigated, the suitable authority must be informed of the investigation. The authority should grant permission for the investigation to be initiated. This will include instruction from an attorney, a police warrant or other effective authorization. The level of authorization required is determined by the type of incident to be investigated.

An internal organization investigation will also require authorization and some form of informed consent from employees. Incidents are often detected covertly and dealt with covertly within an organization. In these instances it is imperative that the organization's policies and procedures are studied to determine any possible investigative limitation.

All the sub-processes listed above build up to the effective deployment of resources to respond to the incident detected. Defects in the sub-processes may be exploited during the following processes of the IDFPM.

Once the incident sub-processes have been completed, the incident response is initiated.

4.4. *Incident response*

The first responders typically arrive at the incident scene. Every investigation is different and it is impossible to determine what the first responders at the scene will encounter. Depending on the type of investigation, witnesses need to be safeguarded, suspects need to be detained as soon as possible after arrival and potential evidence must be secured. The first responder is the first custodian to maintain the chain of evidence and custody of potential digital evidence. The first responder must be able to accurately describe the scene in the initial drafting of documentation; these include photographs, video and sketches (Carrier and Spafford, 2003).

The type of investigation, the known facts and the geographic location of the incident scene determine the approach strategy. An approach strategy is formulated after a brief interview has been conducted with witnesses and/or suspects. The objective of the approach strategy is to initialize a robust chain of evidence and chain of custody, while minimizing possible damage to potential digital evidence.

The location of physical evidence is determined by the approach strategy within the physical world. The digital evidence is located during the search sub-process within the cyber world. Digital evidence can potentially be found at various locations, central or distributed, on different media, depending on the incident.

Searching is limited to determining the exact location of digital evidence ultimately used in the investigation.

Detection and notification determine the primary scene to where the first responders are deployed. The primary scene is usually only an entry point into a broader information system. The encompassing information system is a possible host within which the digital evidence must be located.

Potential digital evidence must be searched for at the incident scene. The incident location can be an initial point, end point or intermediate point in the incident. A perpetrator will usually be at an initial point while a victim is found at an end point. Intermediate points include, but are not limited to, a server used to mask the real attacker, ISPs and routers.

Seizure of digital evidence is dependent on a number of circumstances. A user computer can be packaged easily for transport and storage. A first responder will often encounter an incident within a larger information system. In these instances, the data located after a search should be duplicated immediately. This is in effect an extraction of an exact copy of digital evidence from the incident scene. The physical media is not seized in such instances, but the data is preserved for the purposes of the digital investigation.

Recovery occurs when the original system is restored to a functioning original state with additional security features to prevent similar future incidents (Carrier and Spafford, 2003). This sub-process is not applicable to all types of investigations.

Preservation is the securing, isolation and preserving of the digital and physical state of evidence (Casey, 2004). The seized physical evidence is packaged and then transported to be stored at a suitable location, or alternatively the digital evidence is extracted during collection at the outset of the digital forensic investigation at a digital forensics laboratory. If the digital evidence is not capable of being transported, it must be preserved at the incident scene.

Evidence is transported to a secure location for storage. The integrity, chain of evidence and chain of custody must be accountable during all stages of transportation.

4.5. *Digital forensic investigation*

The physical and digital evidence must be stored in a secure pre-determined location. A standard should be implemented to ensure that the storage location is practical and sufficiently secured for the purposes of storing digital evidence. A selected number of factors should be considered, such as protection against water damage (Casey, 2007), possible malicious activity and theft.

The heart of the IDFPM is the digital forensic investigation. The processes listed will determine the success of the investigator's findings, which will ultimately be presented in court.

The physical investigation process occurs in parallel with the digital investigation if the crime is not isolated to the digital space. The focus of the physical investigation is to analyse DNA, fingerprints and other possible physical evidence obtained from the incident scene. These will not be discussed in this paper.

Collection of digital evidence is where the investigator takes physical possession of the original media. Two bit-by-bit images of the original data are produced by methodically following accepted best practice procedures, ensuring that the original data is not modified. One copy will be the investigation working copy and the other will be preserved in storage to maintain an exact copy of the original evidence.

The result of the collect sub-process is a copy of the original digital evidence, usually on another similar storage media. The digital evidence is a physical copy of the data set, which has no logical data structure. A tool such as Encase will produce a unique file type that will not be readable on most operating systems (Guidance Software, 2011).

The collected data attains legal validity by verifying the extracted data as genuine. A hash value of the original data and copied data is calculated. The hash value of both data sets must be exactly the same. Using a unique one-way hash signature, usually MD5 or SHA-1, authenticates the data.

Examination is generally known to be the process where the investigator makes digital evidence visible or extracts the data into a human readable form. Obfuscated data, which can be deleted or hidden data, is processed using sound digital forensic methods to conduct an effective investigation. With the use of digital forensics tools such as Encase, the sub-process has largely been automated (Guidance Software, 2011).

Once all the data has been rendered visible by examination, the data is harvested by giving a logical structure to the entire data set. The file and folder structure is indexed to give structure to the data collected from the original media. It may well happen that the file allocation tables or disk indexing is deleted in some investigations. The examination process will ensure that files, such as partially deleted files, are recognized from the original evidence medium. The partially discovered files and folders are then harvested. The harvesting process will produce a logical structure; the raw data is represented as information. The partially deleted files processed during examination will be visible to the extent that they were discovered or made visible during examination. Collect, authenticate, examine and harvest will follow in processing sequence. On task level the following will happen: Collection extracts the raw data from the original digital media as bits and bytes. Cohen (2009) states that 'you have a bag of bits' after the data is collected. The raw data is then authenticated and verified, ensuring the copied raw data is a representation of the original data. MD5 or SHA-1 is often used in combination to produce an authentic signature of the original data. The raw data is processed to identify possible metadata traces during examination. Examination is executed by a number of tools, which have the ability to scan for file header and footer data. Harvesting will produce a logical structured data set, where the extracted raw data is now structured information. The harvested information can be mounted and read by the original file system, such as NTFS.

The data analysed in a digital forensic investigation can be quite large. Identifying known data elements reduces the data. Using metadata and unique identifiers, such as MD5, to eliminate known system files and various other application data, does this effectively. The data remaining will be modified data or data that can uniquely be attributed to the users of a specific computer system.

Identification occurs when the investigators use the known digital evidence data to identify a possible incident to be investigated.

During classification, digital evidence with similar identifying patterns is grouped together. Depending on the type of investigation, the data identified should be classified accordingly.

The digital evidence is organized in a manner so as to expedite the digital forensic investigation by focussing on the identified incident type and data classified. The digital evidence is restructured to suitably conduct the identified investigation.

If similar incidents have occurred in the past and are known to the investigator, the known classifications should be used to compare the current digital forensics data with similar past incidents.

Up to this point in the investigation the investigator has only dealt with what is possibly known from the digital evidence. The investigator will have to formulate a hypothesis based on assumptions inferred from the digital evidence by the previous sub-processes. The crux of the hypothesis is to determine a possible root cause of the incident.

During analysis, the organized data is thoroughly investigated and tested against the hypothesis formulated. During this sub-process, the legal validity of possible digital evidence is questioned by considering factors such as relevance, admissibility and weight. Identifying the best possible evidence tests the hypothesis.

When the digital evidence is attributed to a specific user, the digital evidence is linked with a particular individual or event that lies at the root cause of the incident. The findings of the investigator are evaluated to determine whether the hypothesis formulated holds true. When the findings have been evaluated and the hypothesis holds true, the digital evidence is interpreted to produce meaningful statements in the legal context of a technical subject.

A sequence of events inferred from the digital evidence known to the investigator is used to reconstruct a possible event sequence that reflects the incident result as accurately as possible. Reconstruction is not a finding based on the original digital evidence, nor is it established as factual. It is generally used to explain how the incident might have occurred.

The digital evidence and investigator findings are communicated to the relevant interested parties. In most instances this will be the authority that authorized the incident response and subsequent digital investigation.

The investigation results are reviewed and tested against the original hypothesis. Areas of improvement are identified to refine possible findings for the purposes of presentation and reporting. The organization will also determine how to proceed with the incident.

Review is a sub-process through which the investigation is refined. This sub-process can either proceed to the presentation of a report during the presentation process. Alternatively, the hypothesis sub-process forms a cycle that is repeated until the incident can be explained by producing a valid hypothesis with sound relevant admissible digital forensic evidence to support the findings.

4.6. *Presentation*

Presentation occurs when the hypothesis is presented to people other than the investigators, such as a jury or management. A decision will then be made based on the findings.

The presentation of a report involves the compilation of a report detailing the entire investigation process, the chain of evidence, the chain of custody and ultimately the investigator findings that are formulated in an opinion to be presented in court. All other relevant documentation that was compiled during the investigation and that might be relevant in reaching a decision is included in the final presentation report. The legal processes of litigation, if applicable, will become the focus of the processes that follow.

Based on the presentation report, a decision is made regarding the person to whom the incident can be attributed. The decision must be recorded in some database for future reference.

Dissemination is the final activity of the IDFPM. In this subprocess of the investigation, the outcome of the investigation is used to review the exciting policies and procedures of the organization. The original digital evidence is also returned to the rightful owner.

Finally, the IDFPM should not be seen as a static process model. The IDFPM can and must develop and integrate current methods, tools and technologies as they develop. The terminology used must also be expanded to accommodate any of the developments.

5. Conclusion

The paper briefly discussed a number of important definitions that are integral to a digital forensic investigation. Definitions for digital forensic and digital forensic investigations were proposed. Various Digital Forensic Process Models or DFPMs are identified in the current literature. The DFPMs identified all have differing approaches. A selected number of DFPMs were introduced and discussed by listing an adapted process description using sequential logic notation, with the terminology used in each model explained. The DFPMs were compared with each other, and the essential processes required in an integrated digital forensic process model, were identified and abstracted.

In one of the previous sections various problems were identified in the existing DFPMs, such as differing terms that actually refer to the same processes or steps, or the conflicting terminology reflecting different interpretations of a process step. Therefore, the IDFPM is not just a merging of existing DFPMs, but an integration of the discussed DFPMs and a purification of the terminology used, resulting in an all-encompassing standardized IDFPM. The terminology used in the IDFPM is standardized after considering all the process descriptions of the DFPMs discussed.

REFERENCES

Access Data. FTK. Available online at http://accessdata.com/products/computer-forensics/ftk; [last accessed September 2011].

Adelstein F. Live forensics: diagnosing your system without killing it first. Communications of the ACM – Next-generation Cyber Forensics 2006;49(2):63–9.

Baryamureeba V, Tushabe F. The enhanced digital forensic investigation process model. Digital forensics research workshop (DFRWS). Baltimore: Citeseer; 2004.

Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digital forensics research Workshop (DFRWS). Baltimore, St. Paul: West Publishing Co.; 2004. p. 147–67.

Beebe NL. Digital forensic research: the good, the bad, and the unaddressed. IFIP Advances in Information and Communication Technology 2009;306:17–36.

Carrier BD, Spafford EH. Getting physical with the digital forensic process. International Journal of Digital Evidence 2003;2(2).

Carrier BD, Spafford EH. An event-based digital forensic investigation framework. Digital forensics research workshop (DFRWS) 2004.

Carrier BD, Spafford EH. Defining event reconstruction of digital crime scenes. Journal of Forensic Sciences 2004 Nov;49(6): 1291–8.

Carrier BD, Spafford EH. Categories of digital forensics investigation analysis techniques based on the computer history model. Digital Investigation (Elsevier) 2006;3:121–30.

Carrier BD. File system forensic analysis. Addison Wesley; 2005.

Casey E. Digital evidence and computer crime. 1st ed. Elsevier Academic Press; 2000.

Casey E. Digital evidence and computer crime. 2st ed. Elsevier Academic Press; 2004.

Casey E. Handbook of computer crime investigation: forensic tools and technology. 1st ed. Elsevier Academic Press; 2007.

Ciardhua´in SO. An extended model of cybercrime investigations. International Journal of Digital Evidence 2004;3(1). Cohen F. Digital forensic evidence examination. 2nd ed. Fred Cohen & Associates; 2009.

Cohen F. Towards a science of digital forensic evidence examination. In: Kam-Pui C, Shenoi S, editors. Advances in digital forensics VI, IFIP Advances in Information and Communication Technology, vol. 337. Boston: Springer; 2010. p. 17–35.

Garfinkel SL. Digital forensics research: the next 10 yearsThe Proceedings of the tenth annual DFRWS conference. Digital Investigation August 2010;7(Suppl.):S64–73. http://dx.doi.org/10.1016/j.diin.2010.05.009.

Guidance Software. EnCase forensics V7, http://www.guidancesoftware.com/forensic.htm [accessed September 2011].

Ioeng RSC. Forza – digital forensic investigation framework incorporate legal issues. Digital Investigation September 2006:29–36.

Ko¨hn MD, Eloff JHP, Olivier MS. UML modelling of digital forensic process models. Information Security South Africa (ISSA); 2008.

Kruse WH, Heiser J. Computer forensics: Incident response essentials. 1st ed. Addison Wesley; 2002.

Lee HC, Palmer TM, Miller MT. Henry Lee's crime scene handbook. 1st ed. Academic Press; 2001.

Mylonas A, Meletiadis V, Tsoumas B, Mitrou L, Gritzalis D. Smartphone forensics: a proactive investigation scheme for evidence acquisition. In: Gritzalis D, Furnell S, Theoharidou M, editors. SEC 2012, vol. 376. IFIP AICT; 2012. p. 249–60.

Nair BS. Digital electronics and logic design. 6th ed. New Delhi: Prentice Hall; 2006.

Noblitt MG, Pollitt MM. Recovering and examining computer forensic evidence. Forensic Science Communications October 2000;2(4).

Palmer GA. Roadmap for digital forensic research. Digital forensics research workshop (DFRWS) 2001.

Patel A, Ciardhua´in SO. The impact of forensic computing on telecommunications. IEEE Communications Magazine 2000:64–7. Perumal S. Digital forensic model based on Malaysian investigation process. International Journal of Computer Science and Network Security 2009;9(8):38–44.

Pollitt MM. Report on digital forensics. In: 13th INTERPOL forensic science symposium. Computer Analysis Response Team; 2001.

Pollitt MM. A history of digital forensics. In: IFIP international conference digital forensics 2010. p. 3–15.

Robbins J. An explanation of computer forensics. Retrieved 10.02.12, from http://www.pivx.com/forensics.

Rogers MK, Goldman J, Mislan R, Wedge T, Debrota S. Computer forensics field triage process model. Journal of Digital Forensics, Security and Law 2006;1(2).

Rowlingson RA. Ten step process for forensic readiness. International Journal of Digital Evidence 2004;2(3).

Tan J. Forensic readiness. Cambridge, MA: @ Stake. Available online at: http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf; July 2001.

von Solms SH, Louwrens C, Reekie C, Grobler TA. Control framework for digital forensics. In: Sujeet S, Olivier MS, editors. IFIP advances in digital forensics and communication technology. Boston: Springer; 2006. p. 343–55.

Willassen SY, Mjølsnes SF. Digital forensics research. Telektronikk 2005;101(1):92–7. Retrieved from, http://www.telenor.com/telektronikk/ [last accessed on 10.10.08].

Wojcik M, Venter HS, Eloff JHP, Olivier MS. Applying machine trust models to forensic investigations. In: Olivier M, Shenoi S, editors. Advances in digital forensics II, vol. 222. Springer; 2006. p. 55–65.

Wolfe HB. Computer forensics. Computers & Security (Elsevier) 2003;22(1):26–8.

Zachman JA. The Zachman framework for enterprise architecture: primer for enterprise engineering and manufacturing. Zachman International; 2003.

Michael Kohn is currently a candidate advocate in the High Court in South Africa. His main contribution is towards developing the elective presentation of Digital Evidence by way of rigorous internationally accepted Digital Forensics Procedures. He has given testimony in numerous courts. Michael is interested in Trust, Network Forensics, Privacy Encryption, Cyber Forensics, Cyber Crime, Cyber Law and procedural and legal aspects of Digital Evidence. He has a number of conference publications and is involved with the Standardisation of the Digital Forensics Process at the South African Bureau of Standards (SABS).

Mariki M. Eloff received a PhD computer science degree in 2000 from the then Rand Afrikaans University, South Africa, now known as the University of Johannesburg. She is a full professor and chief researcher at the Institute of Corporate Citizenship at Unisa. Prof. Eloff is deputy chair of the Unisa Employment Disability Forum, a council member of The Independent Living Centre for Disabled Persons in South Africa as well as a member of the National Council for Persons with Physical Disabilities in South Africa. In 2010 she received the Unisa Women in Research award for Research Leadership.

Jan Eloff holds a PhD in computer science from the University of Johannesburg, South Africa, previously known as the Rand Afrikaans University. He is currently the Research Director of SAP Research Pretoria specializing in Mobile Empowerment. He is also appointed as an Extraordinary Professor in Computer Science at the University of Pretoria.