Open access • Journal Article • DOI:10.1111/1556-4029.12823

A Comprehensive and Harmonized Digital Forensic Investigation Process Model.

Aleksandar Valjarevic, Hein S. Venter

Institutions: University of Pretoria

Published on: 10 Aug 2015 - Journal of Forensic Sciences (Wiley)

Topics: Digital evidence, Process (engineering) and Digital forensics

A Comprehensive and Harmonized Digital Forensic Investigation Process Model

Aleksandar Valjarevic MSc[1], H. S. Venter Ph.D.[1]

[1] Department of Computer Science, University of Pretoria,

Lynnwood Drive, Pretoria, 0002, South Africa

alexander@vlatacom.com

hventer@cs.up.ac.za

ABSTRACT- Performing a digital forensic investigation (DFI) requires a standardized and formalized process. There is currently neither an international standard nor does a global, harmonized DFI process (DFIP) exist. The authors studied existing state-of-the-art DFIP models and concluded that there are significant disparities pertaining to the number of processes, the scope, the hierarchical levels and concepts applied. This paper proposes a comprehensive model that harmonizes existing models. An effort was made to incorporate all types of processes proposed by the existing models, including those aimed at achieving digital forensic readiness. The authors introduce a novel class of processes called *concurrent processes*. This is a novel contribution that should, together with the rest of the model, enable more efficient and effective DFI, while ensuring admissibility of digital evidence. Ultimately, the proposed model is intended to be used for different types of DFI and should lead to standardization.

Keywords: forensic science, digital forensics, digital evidence, investigation, process, model, harmonization, standardization

Digital forensics gained importance rapidly over the past number of years. Information security incidents are constantly on the rise and are becoming more and more versatile. The fact that societies depend heavily on information technology, contributes to the importance of digital forensics.

Dealing with digital evidence requires a standardized and formalized process in order for digital evidence to be accepted in a court of law. For example, consider the Daubert rule (1), which is most prominently used in the USA for expert witness testimony in digital forensic investigation cases. The Daubert rule clearly states that theories and techniques used to draw conclusions in a case must result in positive answers to a number of questions, notably the question that asks whether the theories and techniques are subject to standards governing their application. Methods and process models for the digital forensic investigation process have been –more often than not– developed mostly by practitioners and digital forensic investigators based on personal experience and expertise, on an ad hoc bases, without the main aim to reach harmonization and standardization within in the field. In the past decade, there were also a number of academic research projects conducted in order to establish a digital forensic investigation process model. By the time of writing this paper, there currently exists no international standard formalizing the digital forensic investigation process. An effort to standardize the process has, however, started within the International Standardization Organization (ISO), by the authors (2). In their previous work, the authors proposed a comprehensive and harmonized digital forensic investigation process model (3,4).

The model proposed in this paper represents further work in achieving comprehensiveness and harmonization. It is important to note that the proposed process model includes processes aimed at achieving digital forensic readiness in order to portray a comprehensive approach to the digital forensic investigation process and achieve the best investigation effectiveness and efficiency. The authors also introduces a novel class of processes called "concurrent processes", defined as the investigation processes that are running in conjunction with other processes within the harmonized process model. These novelties, together with the comprehensiveness of the proposed process model, are important contributions to the field as they represent significant improvements.

The aim of the proposed model and guidelines that are given is to expedite investigations since there would be proper guidelines to guide an investigator through the order of events during an investigation. Such guidelines would also be a good starting point to encourage the training of inexperienced investigators. The provided guidelines should promote guidance on the process to be followed during any kind of digital investigation in such a way that, if challenged in any court of law, no doubt should exist as to the correctness of the investigation process followed during such an investigation. The need for a harmonized digital forensic investigation process model is most prominently experienced within a court of law. In order to be able to claim in court that a standardized set of processes were followed during a digital forensic investigation, would render such cases to be far less susceptible to any discrepancies within the investigation process followed.

The remainder of the paper is structured as follows. Section 1 provides background on digital forensics, legal aspects regarding the digital forensic investigation process, and past work on the digital forensic investigation process. After that, Section 2 presents proposed comprehensive and harmonized digital forensic investigation process. The next section concentrates on the comparison of existing models to the harmonized model. Section 4 concentrates on discussing the comparison performed and characteristics of the proposed mode. Section 5 concludes this paper and gives indications of future work.

Background

The subsections to follow provide background on the following topics. First, background on digital forensics is provided in order to introduce the reader to the basic definition of digital forensics. After that, we provide background on the legal aspects regarding the digital forensic investigation processes, in order to show and emphasize the need for a harmonized and standardized process. The last two subsections in this section present previous work on the digital forensic investigation process and the digital forensic investigation readiness process respectively. The previous work presented in this paper has been used to analyze existing state-of-the-art digital forensic investigation process models and to construct a new comprehensive and harmonized model.

On Digital Forensics

In this section the authors provide a definition of digital forensics as assembled from various sources within previous research by the authors. The digital forensic investigation process is defined as the use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation and distribution and/or return and/or destruction of digital evidence derived from digital sources, while obtaining proper authorizations for all activities, properly documenting all activities, interacting with the physical investigation, preserving the evidence and the chain of custody, for the purpose of facilitating or furthering the reconstruction of events found to be incidents requiring a digital forensic investigation, whether of criminal nature or not. (2)

Legal Aspects

In this section the authors provide an overview of the legal aspects pertaining to digital forensics and especially the admissibility of digital evidence in a court of law. This overview is not comprehensive but aims to provide the reader with a sense of the need for a harmonized, and ultimately, a standardized digital forensic investigation process. Legal requirements may differ extensively in different jurisdictions across the world. The premise of this section is not to advocate specific legal systems, but rather to note the generic requirements in terms of legal issues that can be adopted by the legal system of any jurisdiction. For example, in the United Stated of America criminal cases that include the presentation of digital evidence are treated under rule 702 of the Federal Rules of Evidence, which says: "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise." For application of this rule, the Daubert rule (1) is the most important. Other countries have similar guidelines regarding the admissibility of digital evidence (5, 6, 7, 8). Requirements for admissibility may vary considerably between jurisdictions and for that reason it is highly advisable to obtain competent legal advice regarding the particular jurisdiction’s specific requirements.

The next section gives an overview of work on the digital forensic investigation processes thus far.

Related Work on Digital Forensic Investigation Process Models

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 (9), the need for a standard framework for digital forensics has been widely acknowledged (10-16). The digital forensic investigation process model proposed at this workshop includes the following seven processes: Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision. The process model was defined as iterative.

Reith et al. (10) proposed a digital forensic investigation process model known as the abstract model, which includes the following processes: identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning evidence.

The U.S. Department of Justice (DOJ) published a process model in the Electronic Crime Scene Investigation Guide aimed at first responders (11). This proposed process model includes the following processes: preparation, recognition and identification, documentation of the crime scene, collection and preservation, packaging and transportation, examination, analysis and reporting.

Carrier and Spafford (12) propose a process model based on the following requirements: The model must be based on existing theory for physical crime investigations; The model must be practical and follow the same steps that an actual investigation would take; The model must be general with respect to technology and not be constrained to current products and procedures; The model must be specific enough that general technology requirements for each process can be developed; The model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response. The model proposed by Carrier and Spafford (12) includes 17 processes organized into the following five groups: readiness processes, deployment processes, physical crime scene investigation processes, digital crime scene investigation processes and review process. Carrier and Spafford (18) also proposed another (similar) event-based process model. This model is, again, based on physical crime investigation and it is suggested that digital crime scene investigation should occur as a subset of a physical crime scene investigation. The paper concentrates on digital crime scene investigation processes and how to find the causes and effects of events during a digital forensic investigation.

Mandia et al. (13) proposed a digital forensic investigation process known as the incident model, which contains the following processes: pre-incident preparation, detection of the incident, initial response, response

strategy formulation, duplication (system backup), investigation, secure measure implementation (isolation and containing the suspect system), network monitoring, recovery (recovery of the suspect system to original process), reporting and follow-up.

Beebe and Clark (14) proposed a hierarchical, objectives-based digital forensic investigation process model and also drew a comprehensive comparison between their proposed process model and previous works in this field. The model they proposed is multi-tiered, which constitutes a novel approach. First-tier processes proposed in (14) include the following: preparation, incident response, data collection, data analysis, findings presentation and closure. In their opinion, second-tier sub-processes should be defined in such a way that these are inclusive of all possible types of crime and types of digital evidence.

Cuardhuáin (15) proposed an extended and comprehensive model of cybercrime investigations, which is very comprehensive. The harmonized model also includes information flow description between different processes.

Casey and Rose (16) define processes of digital forensic investigation process as: gather information and make observations, form a hypothesis to explain observations, evaluate the hypothesis, draw conclusions and communicate findings.

Cohen (17) proposed a process model that includes the following processes: identification, collection, preservation, transportation, storage, analysis, interpretation, attribution, reconstruction, presentation and destruction. Cohen et al. (19) discuss the state of the science of digital evidence examination and consensus in digital evidence examination. He recognizes that numerous calls have been made for scientific approaches and formal methods in the field of digital forensics.

As previously mentioned, in the United Kingdom, examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and integrity of evidence (5, 6). These guidelines do not explicitly set out the digital forensic investigation process model, but, through recommendations, the given process model can be constructed, containing following processes: preparations for investigation, crime scene group of processes, secure and control the crime scene, photograph and document the scene, initial collecting of volatile data, attaching exhibit labels, documenting each action performed,

transportation, storage, evidence recovery group of processes, the collection process, the examination process, the analyses process, the reporting process, disclosure.

Based on related work on the digital forensic investigation process, the authors of this paper conclude that there are significant disparities among existing digital forensic investigation process models. Disparities pertain to the number of processes included, the scope of models, and the scope of similarly-named processes within different models, the hierarchy levels and even concepts applied to the construction of the model (i.e. some of the models are based on the physical crime investigation processes). The authors also note that they are of the opinion that the body of knowledge and peer-reviewed papers on the digital forensic investigation process are scarce and those experts and practitioners in the field should concentrate more on this subject. An effort to standardize the process has, however, started within the International Standardization Organization (ISO), by the authors (2). This international standard provides guidelines that encapsulate idealized models for common investigation processes across various investigation scenarios (2). The research presented in this paper presents important input to the development of the standard. ISO/IEC 27043 is intended to complement other standards and documents which provide guidance on digital forensics investigation process.

Related Work on Digital Forensic Readiness Investigation Process Models

This section provides an overview of past work on digital forensics investigation readiness (DFIRP).

Digital forensic readiness is defined as the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation (20). What follows is a brief overview of work related to the digital forensic readiness processes.

Tan (20) identified factors that affect digital forensic readiness: how logging is done; what is logged; Intrusion Detection Systems (IDSs); digital forensic acquisition; digital evidence handling.

Yasinac and Manzano (21) propose six categories of policies to facilitate digital forensic readiness: retaining information; planning the response; training; accelerating the investigation; preventing anonymous activities; protecting the evidence.

Wolfe-Wilson and Wolfe (22) emphasize the need for an organization to have procedures in place in order to preserve digital evidence in the event that a digital forensic investigation (DFI) is needed.

Rowlingson (23) defines a number of goals for digital forensic readiness as follows: To gather admissible evidence legally and without interfering with business processes; To gather evidence targeting the potential crimes and disputes that may adversely impact an organization; To allow an investigation to proceed at a cost in proportion to the incident; To minimize interruption to the business from any investigation; To ensure that evidence makes a positive impact on the outcome of any legal action. Rowlingson also defines key activities in the implementation of digital forensic readiness and this is, in the opinion of the authors, the closest to our defined DFIRP model: Define the business scenarios that require digital evidence; Identify available sources and different types of potential evidence; Determine the evidence collection requirement; Establish a capability for securely gathering legally admissible evidence to meet the requirement; Establish a policy for secure storage and handling of potential evidence; Ensure monitoring is targeted to detect and deter major incidents; Specify circumstances when escalation to a full investigation should be launched; Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence; Document an evidence-based case describing the incident and its impact; Ensure legal review to facilitate action in response to the incident.

There are several works presenting digital forensic models, which include readiness as a process as discussed above, but, to the best knowledge of the authors, there is no DFIRP model proposed. Our harmonized model includes the DFIRP model, as a part of a comprehensive digital forensic investigation process (DFIP) model. The methodology used to propose a comprehensive harmonized digital forensic investigation process model is discussed next.

A Comprehensive and Harmonized Digital Forensic Investigation Process Model

In this section the authors present the proposed digital forensic investigation process model.

The digital investigation process model consists of several sub processes. Each of these processes are generic enough and described at such a level of abstraction in this paper so that they can be used for different types of digital forensic investigations and for different types of digital evidence. Also, the model is

comprehensively harmonized, meaning that it is inclusive of the benefits of all the previous models examined during this research. The new harmonized model inherits most of the processes proposed by other authors and introduces additional processes and, in that sense, it is comprehensive. It proposes a harmonized organization of the processes while introducing a novel approach in the way some of the processes have been implemented, i.e., *concurrent processes*. We define concurrent processes as the principle actions which should be achieved in parallel with other processes within the digital forensic investigation process model. The authors believe that the introduction of a class for concurrent processes is a significant contribution, which would enable more efficient and reliable investigations to take place as well as promote strict adherence to the digital forensic investigation principles.

Processes have been selected based on previous work in this field. An attempt was then made to harmonize the processes described by other authors and organizations. The following principle was used to distinguish between different processes: A set of activities can be defined as a process if all activities have a common aim and if activities last for a limited period of time (3).In order to abstract all processes on a higher level, all digital forensic investigation processes in the harmonized model are categorized into the following digital forensic investigation process classes (2): Readiness processes class, Initialization processes class, Acquisitive processes class, Investigative processes class and Concurrent processes class.

These classes are discussed in the following subsections starting with an overview of the proposed classes first. We start with an overview in order for the reader to gain a holistic view of the model and its classes first. In addition, one should also then be able to understand basics about each of the classes as well as how these classes relate before drilling into the details.

Overview of the digital forensic investigation process classes

In order to abstract the digital investigation processes at a higher level, these processes can be categorized into the following digital investigation process classes. Figure 1 shows the classes of digital forensic investigation processes and an overview of their relations.

The readiness class of processes deals with pre-incident investigation processes aimed at reaching digital forensic investigation readiness within an organization. The processes in this class attempt to maximize the use of potential digital evidence, while minimizing the costs and interference with business processes. This class of

processes should also enable preserving or improving the information security of potential digital evidence. Note that the readiness processes are optional to the rest of the digital forensic investigation processes. The reasons for this are explained in more detail in section 2.2; however, the main reason why the readiness processes are optional is due to the fact that the readiness processes are proactive compared to the rest of the investigation processes, which are re-active in nature. The next three classes include the *initialization processes, acquisitive processes and investigative processes* respectively. All these classes follow one another and do not overlap in time. As shown in Figure 1, however, the *concurrent processes* class runs in parallel with all other classes, ensuring the application of digital forensics principles.

The initialization class of processes deals with the initial commencement of the digital forensic investigation. The processes in this class are concerned with incident detection, first response, planning and preparation of the actual digital forensic investigation. These processes are of extreme importance for the success and effectiveness of the investigation, as these represent the basics and foundation for any of the processes following the initialization processes. If any error or omission is made during these processes digital evidence might become unusable or unavailable and complete process integrity might be endangered. For example if during first response, first responder shuts down a computer containing digital evidence, digital evidence from RAM memory might be lost, or if one does not prepare for potential digital evidence collection and acquisition investigation can encounter difficulties at later stages (loss of time, resources or even potential digital evidence.

The acquisitive class of processes deals with the physical scene investigation of a case. Processes in this class are concerned with acquisition of digital evidence. The validity and relevance of digital evidence depend heavily on these processes, as during these processes one deal with digital evidence and might compromise its integrity or might overlook important evidence.

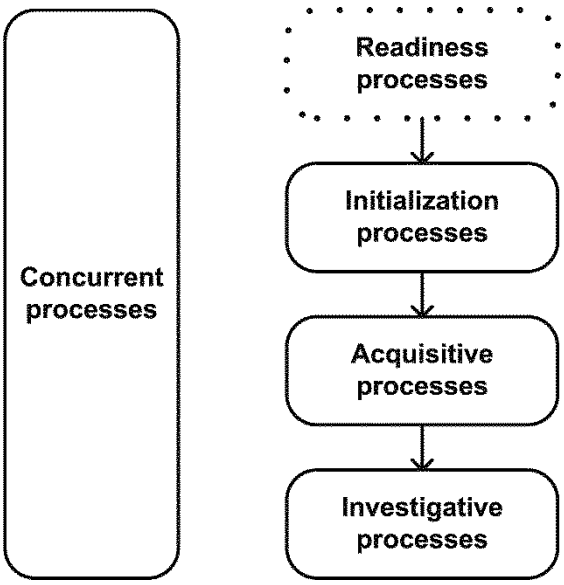

Fig. 1. The classes of the proposed model

The concurrent class of processes takes place concurrently with all the other processes mentioned above. Concurrent processes are defined as the principles which should be applied throughout the digital forensic investigation process since such concurrent processes are applicable to many other processes within the digital forensic investigation process. These processes are important as they ensure that digital forensic principles are implemented and abided by, ensuring proper digital evidence admissibility and greater investigation effectiveness. The concurrent processes are aimed at achieving the highest possible efficiency of the investigation and to ensure the admissibility of digital evidence. Translating these principles into actionable items makes it easier for practitioners to strictly adhere to them.

The following subsections provide brief explanation each of the digital forensic investigation process classes mentioned above.

Readiness processes

Overview of the readiness processes

This class of processes, as mentioned before, is optional to the digital forensic investigation processes and is affected by an organization rather than the investigator(s). It should be mentioned that future legislation (in

applicable jurisdictions) and/or corporate governance guidelines might enforce organizations to implement the readiness processes as well, due to the rise in the number of cyber attacks across the world. In their effort of harmonizing, the authors have adopted and defined the following aims for a readiness processes class, which are harmonized mostly from previous work (Carrier and Spafford, 2003; Carrier and Spafford, 2005; Mandia et al., 2003; Beebe and Clark, 2005; Tan, 2001; Yasinac and Manzano, 2001; Wolfe-Wilson and Wolfe, 2003; Rownlingson, 2004), except for the last aim, which was added by the authors. The processes in this class should:

1. Maximize the potential use of digital evidence;
2. Minimize the costs of digital forensic investigations incurred;
3. Minimize interference with and prevent interruption of business processes;
4. Preserve or improve the current level of information security.

The authors firmly believe that aim 4 should also be taken into account when implementing readiness measures. It is not viable to only concentrate on efficiency of the investigation (aims 1 and 2) and non-interference with business processes (aim 3), because having only the first three aims could still leave room for flaws in the overall information security status of an organization. An example of such a flaw is when an organization, based on the first three aims, decides to collect logs from its information systems keeping it at a central location, but does not envisage security mechanisms for sufficiently protecting that data at the central location, which might lead to the compromise or leakage of that data. It is, therefore, necessary to take a more holistic approach by applying the CIA information security principles as mentioned earlier. The authors believe that the harmonized model should have built-in security features and security should not merely be an add-on.

Figure 2 depicts the readiness processes class as described above, refined into process groups as follows. The class of readiness processes consists of three distinctive readiness process groups, being the *planning process group*, the *implementation process group* and the *assessment process group*, as shown in Figure 2.

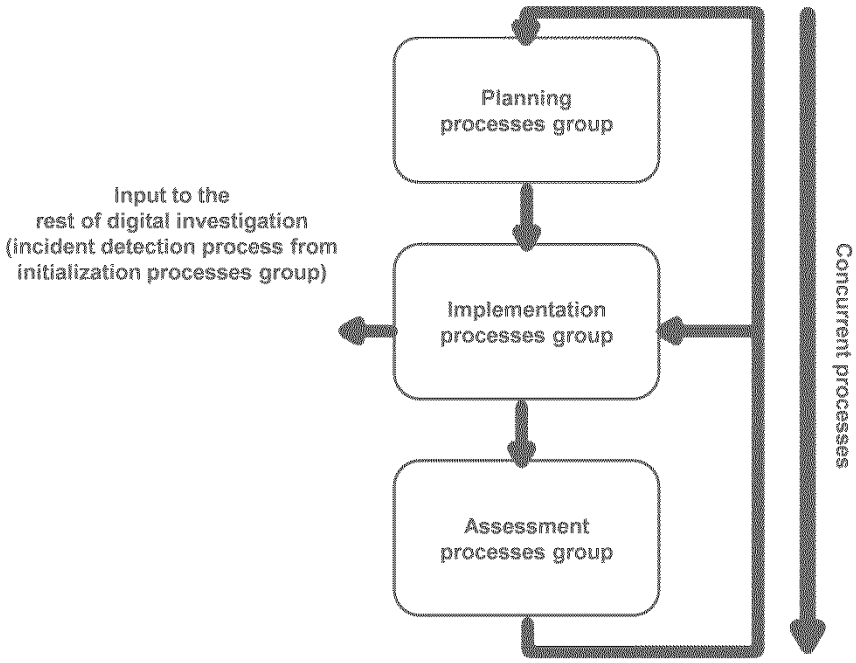

Fig. 2. Readiness processes groups

The planning processes group includes all readiness processes that are concerned with planning activities, including scenario definition, identification of potential digital evidence sources, planning pre-incident collection, storage and handling of data representing potential digital evidence, planning pre-incident analysis of data representing potential digital evidence, planning incident detection, and defining system architecture, as all depicted in Figure 3.

The implementation process group includes the following readiness processes: implementing system architecture, implementing pre-incident collection, storage and handling of data representing potential digital evidence, implementing pre-incident analyses of data representing potential digital evidence and implementing incident detection, as shown in Figure 3. These processes are concerned with the implementation of the results of the planning processes.

The assessment process group includes two readiness processes, the assessment of implementation and the implementation of assessment results. The *implementing incident detection* process links to the *incident detection* digital forensic investigation process as shown in Figure 7.

Note that the processes are defined at a high level in order to be used as a model for different types of Digital Forensic Investigations (DFIs). The authors do not attempt to prescribe what exactly each of the processes

should entail. There exist many different types of DFIs, such as live forensics, cloud forensics, network forensics and mobile forensics. We believe that detailed procedures for each subsequent process should be defined for each specific type of DFIs, however, doing so is not within the scope of this paper. The harmonized model should, therefore, be used as an 'umbrella' model for each of the different DFI types, i.e. the detailed procedures are to be implemented by other standards and DFI practitioners.

Input to all processes in Figure 3 includes all information regarding system architecture, technology (hardware and software), policies, procedures and business processes of an organization where applicable. The input must also consider the four aims for the readiness processes as mentioned earlier. The input arising from the mentioned four aims are referred to as pre-known system inputs in the remainder of the paper. For example pre-known system inputs may include, amongst others, network topology of the system, specification of models and components of hardware used, specification of firmware, operating systems and applications for each piece of hardware (if applicable for the hardware in question), information security policies that are in place regarding the use of system and description of business use of the system in question.

The readiness processes are iterative, which implies that, after the last process, one can return to previous readiness processes, as shown in Figure 3. For example, when, during the *assessment of implementation* process, one notes that certain defined system architecture has not been properly implemented, one would need to go back to the *implementing system architecture* process. Another example is if one notes that plans made during the *planning pre-incident collection, storage and handling of data representing potential digital evidence* process are not in line with aims for having digital forensic investigation readiness processes in the particular organization, one could go back to the *planning pre-incident collection, storage and handling of data representing potential digital evidence* process in order to change those plans accordingly.

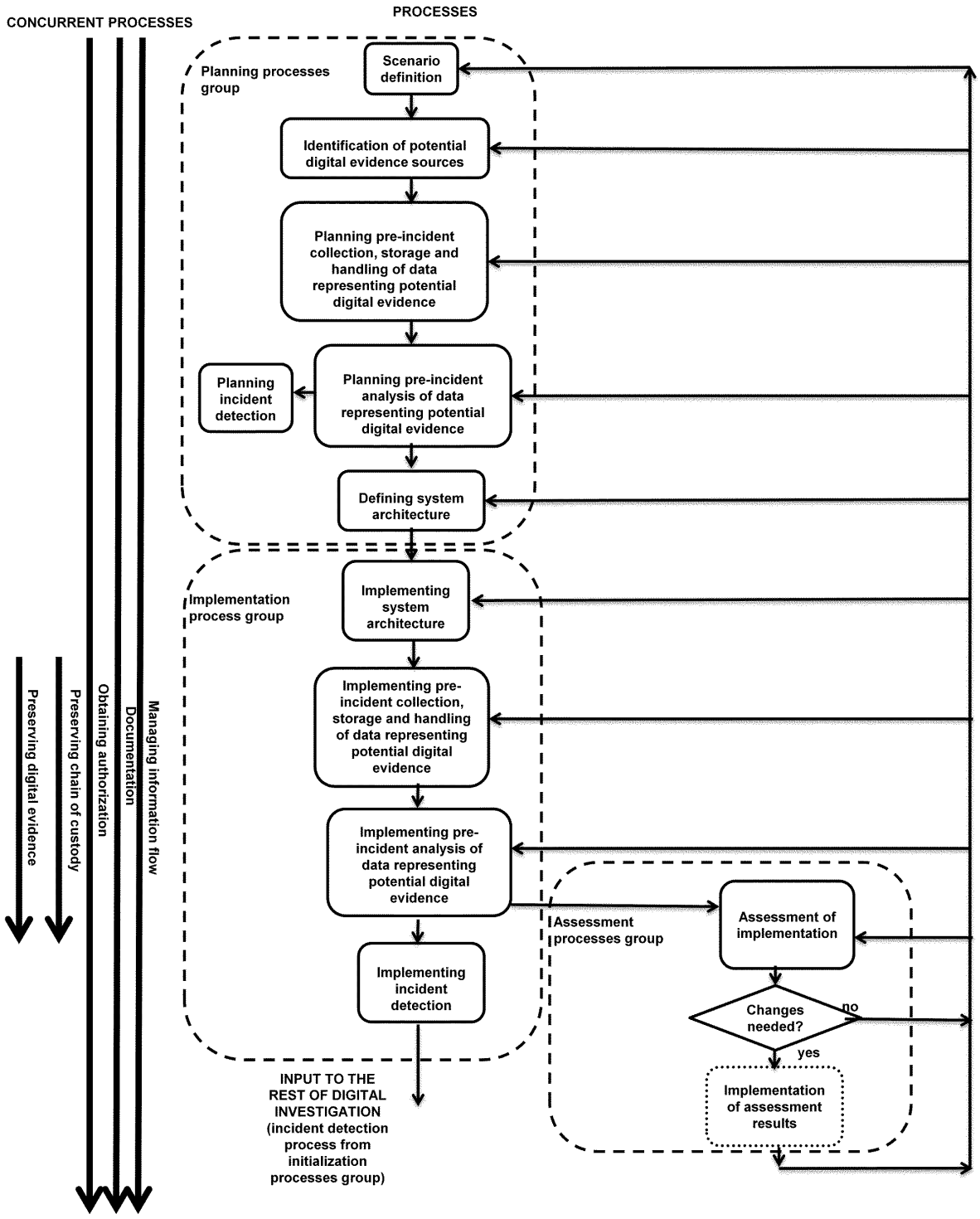

Fig. 3. Readiness processes

Each of the readiness processes are explained in the clauses that follow.

Scenario definition

In this process one should examine all scenarios where digital evidence might be required. The output of this process includes the defined scenarios. These might be scenarios of information security incidents, such as unauthorized use of resources. These can also be scenarios of other events that, as a consequence, require a digital forensic investigation, such as investigating the use of a computer to distribute child pornography.

It is also recommended that a proper risk assessment is performed during this process for each identified scenario respectively. A risk assessment would enable one to better identify all possible threats, vulnerabilities and related scenarios that would expose particular information assets. Based on the assessed risk from certain threats, vulnerabilities or scenarios, one can, in later processes, better decide on the required controls to achieve investigation readiness within an organization. This will enable an organization to take into account the risk level, costs, and benefits of possible controls in a bid to reduce the identified risk.

The *scenario definition process* is a logical start for the *readiness processes class*, as it enables one to lay the foundation needed for all further process through proper scenario analyses. After this initial process one should define all possible sources of digital evidence, based on the scenarios defined within this process. The *sources identification process* is again a prerequisite for further processes, which deal with handling potential digital evidence.

Identification of potential digital evidence sources

In this process one should identify all potential sources of digital evidence within an organization. The output of this process is the defined potential sources of digital evidence. Some of the identified potential sources might not be available. For example, if access logs are not introduced within the system, it means that access logs will not be available as a source of data in the case of a digital forensic investigation. In that case, controls should be explored to make the identified source available.

After the potential digital evidence sources have been identified, one should define/determine how these sources would be handled. Therefore, the next two processes include the *planning pre-incident collection,*

storage and handling of data representing potential digital evidence and the *planning pre-incident analysis of data representing potential digital evidence*. These processes are explained in the next two sub-sections, respectively.

Planning pre-incident collection, storage and handling of data representing potential digital evidence

In this process one should define activities for pre-incident collection, storage and handling of data representing potential digital evidence. The output of this process includes the defined activities for pre-incident collection, storage and handling of data representing potential digital evidence.

The collection period of data is to be determined by a risk assessment. For example, this could mean determining how often an organization would save the application log to a central repository, in order to ensure integrity of the log data in case that the application is compromised. Also, note that the collection, storage and handling of data have to conform to digital forensic investigation principles in order for digital evidence to be admissible in a court of law. Lastly, the retention period of data is to be determined based on the following factors:

- risk assessment;
- previous experience regarding incident detection, data quantities, network capacity and all other matters that could influence cost or efficiency of this process;
- laws within the particular jurisdiction;
- regulations;
- business-specific requirements.

Planning pre-incident analysis of data representing potential digital evidence

In this process one should define procedures for pre-incident analysis of data representing potential digital evidence.

The input to this process includes the scenarios as defined in the scenario definition process as well as the output from the pre-incident collection process. The input must also include the aims for the readiness processes.

The output of this process includes the defined activities for pre-incident analysis of the data that represent potential digital evidence. The aim of this analysis is to detect an incident. Therefore, activities defined in this process must include exact information on how the incident is detected and what behavior constitutes an incident. As the output of this process is delivered in the form of detected incidents, this links to the input of the incident detection process of the digital forensic investigation processes as listed in Figure 3.

As the task of data analysis and incident detection is often outside the scope of the functionalities of targeted information systems, it is recommended that this process defines an interface between the readiness processes and a monitoring system, which would analyze data in order to detect incidents. The monitoring system can be any system that is specialized for this purpose. It can also be any one of the following systems: intrusion prevention systems, intrusion detection systems, change tracking systems, log processing systems etc.

Planning incident detection

In this process one should define actions to be performed when an incident is detected. The output of this process includes defined actions to be performed once an incident is detected, in particular information to be passed on to the rest of digital forensic investigation process. Information should also include pre-known system inputs, results from all of the readiness class processes as well as data gathered and generated during the *implementation process group* processes.

Defining system architecture

In this process one should define information system architecture for the organization, while taking into account the output results of all previous readiness processes. We introduce this process in order to enable better results of the DFIR implementation, through taking into account all relevant matters when redefining the system architecture.

Input to this process is the results from all previous readiness processes. The input must also include the aims for the readiness processes.

The output of this process is the defined system architecture for the organization. The aim is to customize system architecture to accommodate the accomplishment of the aims of the readiness processes.

After we have defined the system architecture, one should embark on implementation of conclusions and results from all of the processes performed.

Therefore, after this, one should proceed with processes from the *implementation process group*.

Implementing system architecture

In this process one should implement the system architecture as defined in the *defining system architecture* process. The output of this process is the implemented system architecture. Examples of *implementing system architecture* include the installation of new software, hardware and/or policies which will permit the remainder of the readiness processes to be instantiated across the information system and the organization.

Implementing pre-incident collection, storage and handling of data representing potential digital evidence

In this process one should implement pre-incident collection, storage and handling of data representing potential digital evidence, as defined in the *planning pre-incident collection, storage and handling of data representing potential digital evidence* process. The output of this process is the implemented pre-incident collection, storage and handling of data representing potential digital evidence.

Examples of *pre-incident collection, storage and handling of data representing potential digital evidence* include the implementation of logging software and hardware, with time stamping and digital signature mechanisms in place, or the implementation of customized software to collect the data of importance (i.e. system usage data).

Implementing pre-incident analysis of data representing potential digital evidence

In this process one should implement pre-incident analyses of data representing potential digital evidence, as defined in the *planning pre-incident analyses of data representing potential digital evidence* process. The output of this process is the implemented pre-incident analyses of data representing potential digital evidence.

Examples of *pre-incident analyses of data representing potential digital evidence* include the implementation of change-tracking software, intrusion detection/prevention software and/or anti-virus software.

Implementing incident detection

In this process one should implement the actions defined in the *planning incident detection* process. The implementation of incident detection depends also on and receives input from the *implementing pre-incident analyses of data representing potential digital evidence* process, as detection occurs based on the analyses performed.

During the *implementing incident detection* process, detection of an incident occurs according to the rules defined during *planning incident detection* process. Also, during the *implementing incident detection* process, one should decide on which data about the incident should be passed on to the rest of digital forensic investigation process.

Examples of incident detection can be if change tracking software detects changes in a certain archived log or if an intrusion is detected via intrusion detection system.

Requirements for an event to be declared an incident requiring digital forensic investigation would depend on policies of organization and cannot be prescribed by this paper.

This process represents an interface to the rest of the digital forensic investigation process. This process is an overlap between readiness processes and an investigation itself. The reason for overlap is that the digital forensic investigation cannot start until there is an incident detected.

Assessment of implementation

In the *assessment of implementation* process, one performs an assessment of the results of the *implementation process group* and compares these to the aims for achieving digital forensic investigation readiness.

The output of this process is the results of the assessment of implementing digital forensic investigation readiness for an information system. It is recommended that, at this process, a legal review is carried out for all procedures, controls and architectures defined previously. The review should show, amongst other, whether there is conformity with the legal environment and digital forensics principals of the particular jurisdiction, in order to ensure admissibility of potential evidence in court.

Implementation of assessment results

This process is concerned with the implementation of the conclusions from previous process.

Note that this process is optional, as it is possible that no changes are needed, based on the *assessment of implementation* process.

In Figure 3, this process is marked as optional and indicated as such with a dashed line around the process.

During this process one should decide on recommendations for changes in one or more of the previous processes. The main decision here is whether to go back to one of the planning processes in the *planning processes group* of the *readiness class* of processes or to go back to one of the processes in the *implementation process group,* depending on the conclusions of the *assessment of implementation p*rocess. For example, one might conclude that the implementation of a certain measure (i.e. that during *implementing system architecture,* one has not properly implemented log-in authorization controls planned during the *defining system architecture* process) was not performed in an optimal manner, or one might decide that new implementation as to be performed.

Initialization processes

Overview of initialization processes

This class of processes is dealing with the initial commencement of the digital forensic investigation including *incident detection, first response, planning* and *preparation processes*.

Incident detection process

Incident detection procedures must be in place prior to the beginning of this process. The procedures can define the relation between the information system where the incident might occur and the external information system, which would have the task to detect an incident or can define how humans operating or administering information systems, detect an incident. Examples of external incident detection systems are intrusion detection systems, intrusion prevention systems, log-analyzing systems, change-tracking systems, etc.

The incident detection process includes not only the detection of the incident, but also the classification and description of the incident, which has a significant influence on the rest of the process. For example, the digital forensic investigation would take a completely different course if the incident was described as 'unauthorized access to the root account of the operating system', than if it was described as 'using the computer to distribute abusive images'. Based on the above, this process may consist of three sub-processes: incident detection, incident classification and incident description. It is important to note that the incident classification and incident description sub-processes should be performed based on information gathered prior to incident detection and should not include any activity (i.e. running some data analyses software on the system) that might alter data at the information system in which incident has occurred, in order to preserve digital evidence.

Incident detection activities were defined since DFWRS (9) (as part of Identification process), but Mandia et al. (13) were the first to define these in separate process/process. The authors strongly believe that incident detection activities should be included in digital forensic investigation process, as a starting point. The reasoning behind selecting incident detection process as a first process in the model and not a preparation or planning process, as some authors have suggested is that we believe that digital forensic readiness activities should exist in a process separate to a digital forensic investigation process, as digital forensic practitioners could never insure that each system they will be working on can have digital forensic readiness activities implemented. (If preparation and planning for digital forensic investigation would exist prior to incident detection then this would be part of digital forensic readiness.) Therefore, the actual digital forensic investigation starts with *incident detection* and *first response*, followed by *preparation* and *planning* processes.

First response process

The *first response* process should include the first response to the detected incident. Depending on the type and severity of the incident, this might include disconnecting equipment from a networked environment, detecting corrupted data, etc. It is required that the first response does not have a negative influence on the possibility to perform a digital forensic investigation, e.g. to avoid powering off the equipment, opening or changing files on a live system etc. Defining the *first response* sub processes is out of the scope of this document, as these can vary greatly depending on the type of target information systems, data contained in the target information system, circumstances of the incident, classification and description of the incident, etc. Mandia et al. (13) and Beebe and Clark (14) have included incident response process in their models as initial response and incident response, respectively. The authors have chosen to include this process because we firmly believe that it must be part of digital forensic investigation process in order to ensure integrity of digital evidence. (i.e. so it does not happen that first responder destroys or alters some of the digital evidence, i.e. application configuration files).

Planning process

During this process the investigator has to perform all the potential planning needed for later in the digital forensic investigation process. Planning should include the development of relevant procedures, the definition of methodologies and tools to be used, planning for use of appropriate human resources and the planning of all activities during other processes. If digital forensic investigation readiness controls were implemented, the investigator should plan how to use the results of those controls so as to maximize the success of the digital forensic investigation process. The aims of the digital forensic investigation readiness process are to maximize the potential use of potential digital evidence, minimize the costs of the investigation, minimize interference with and prevent the interruption of business processes, and to preserve or improve the current level of information systems security. The planning process is included because it is of extreme importance due to the fact that it determines the efficiency and success of all the other processes.

Preparation process

Preparation process activities are intended to prepare an organization for performing the activities of other digital forensic investigation processes. This might include – but is not limited to – the preparation of relevant equipment (hardware and software), infrastructure, human resources, raising awareness, training and documentation. During this process, preparations also have to be made to implement procedures defined in the previous process. This process is included since such a process will ensure that the investigator is better prepared in order to carry out the acquisitive processes in a more efficient manner. This will also ensure that the integrity of potential digital evidence is not compromised due to possible ill preparedness by the investigator.

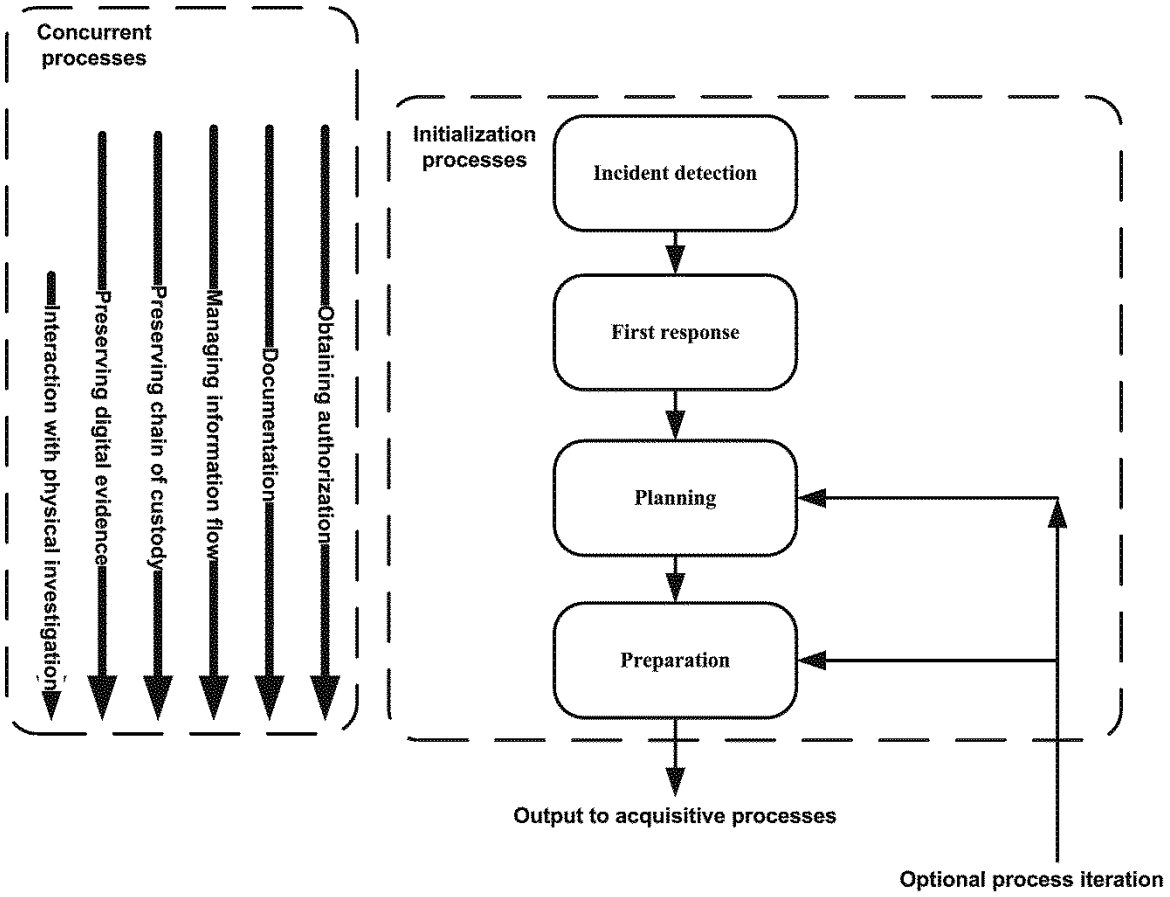

Fig. 4. Initialization processes

Acquisitive processes

The acquisitive processes class consists of processes that are concerned with acquisition of digital evidence, as shown in Figure 5.

Potential digital evidence identification process

This is the first process performed at the scene of the incident. Although it overlaps in time with the previous process, it should be considered as a separate process because it includes different types of procedures within the process, with the specific aim of identifying potential digital evidence. Cohen says in (17): “In order to be processed and applied, evidence must first, somehow, be identified as evidence. It is common for there to be an enormous amount of potential evidence available for a legal matter, and for the vast majority of the potential evidence to never be identified.” Identifying potential digital evidence at the incident scene is of crucial importance for the remainder of the process, because if potential digital evidence is not identified at this point, it might not even exist at a later point during the process. This is especially important when an incident happens in a networked environment, in an environment where live investigations should be performed, in a cloud environment or in an environment with exceptionally large amounts of data to deal with. (6, 10, 11, 12, 15, 16, 17) have included this process in their respective models, some with different name and with different scope. The authors believe that *Potential digital evidence identification process* should be a separate process, with sole aim to identify potential evidence.

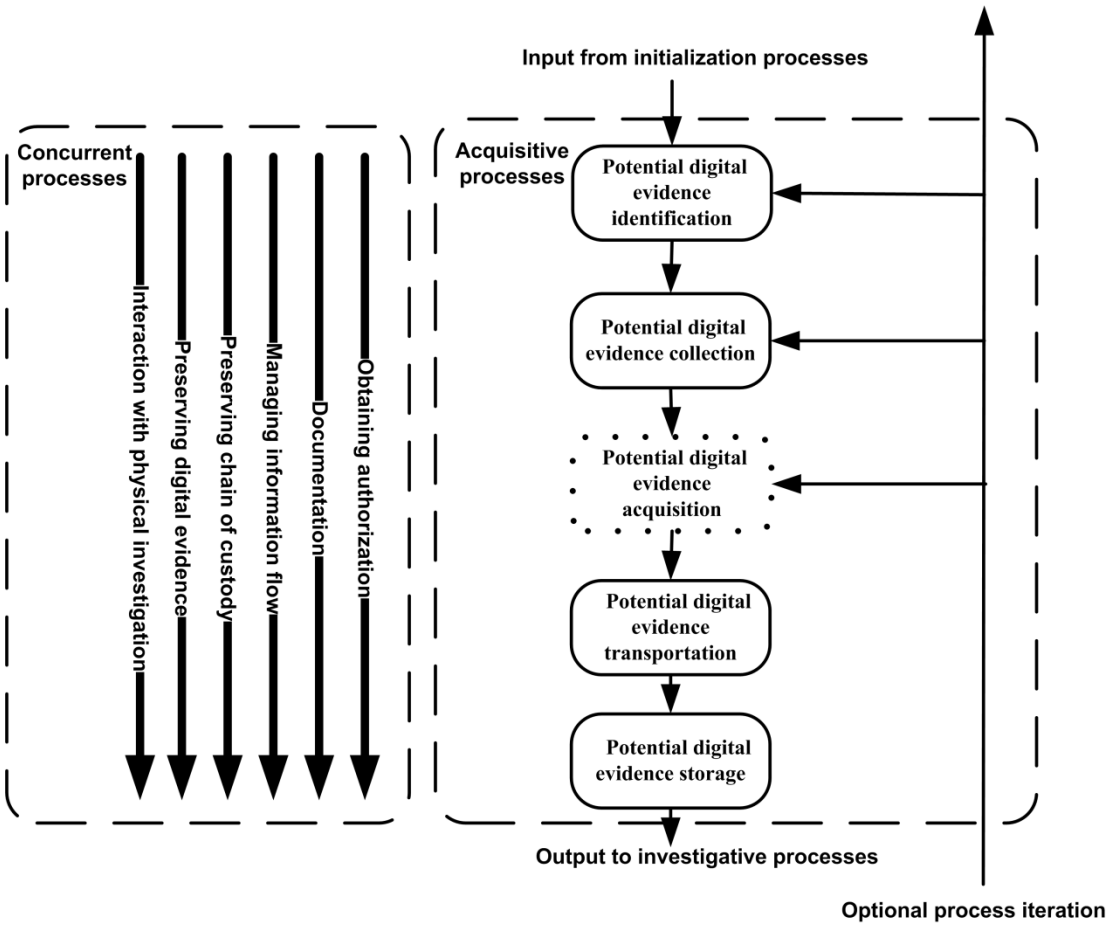

Fig. 5. Acquisitive processes

Potential digital evidence collection identification process

Once potential digital evidence has been identified, it has to be collected in order to permit its analysis in a later process. Evidence must be collected in such a manner that its integrity is preserved. This is important if one needs to use this evidence at a later stage to draw some formal conclusions, i.e. in a court of law. Adhering to strict legal regulations during the evidence collection process is of crucial importance, as digital evidence might become unusable when proper procedures are not followed. It is notable that many authors (9, 10, 17) have proposed two separate processes instead of our c*ollection process*. Namely, they propose a separate collection

and preservation processes. However the authors believe that this should be a single process as the aim is simply to collect potential evidence. Preserving the evidence, on the other hand, is more of a principle to be followed.

Potential digital evidence acquisition process

Once potential digital evidence has been collected, it has to be acquired in order to permit its analysis in a later process (2). Again, adhering to strict legal regulations during the potential digital evidence acquisition process is of crucial importance, as potential digital evidence might become unusable when proper procedures are not followed. Take note that this process is optional at this stage, since it is not always possible to acquire one or more images of the evidence after it has been collected. It often happens that the image acquisition only takes place within an investigation laboratory and, hence, this process might only occur within the investigative processes class (2).

Potential digital evidence transportation process

During this process, potential digital evidence is to be transported to a location where it is to be stored and later analyzed. Transportation can be done physically or electronically. If the evidence is transported electronically, special precautions have to be taken to preserve the integrity and chain of custody, such as encrypting and digitally signing data. In various sources (11, 15, 16) this is included as a separate process. This should exist as a separate process on a basis that activities performed have a single aim, not shared with other processes, to securely transport the potential evidence to the location where analyses would be performed, while obliging to principle of preserving the evidence.

Potential digital evidence storage process

The storage of potential digital evidence might be needed if analysis cannot be performed right away or if there is a legal requirement to keep digital evidence for a certain period of time. Preservation of the integrity of the evidence and the chain of custody is of utmost importance during this process. Care must also be taken not to damage the media containing potential digital evidence due to shock, temperature, humidity, pollution, loss of power, malfunction, etc. In various sources (6, 15, 17) this is included as a separate process. This should exist as

a separate process on a basis that activities performed have a single aim, not shared with other processes, to securely and safely store the potential evidence.

Investigative processes

Overview of investigative processes

The *investigative processes class* consists of processes that are concerned with investigating the incident that is the cause of the digital forensic investigation and is concerned with analyzing the evidence, interpreting results from the analyses, writing the report on results of the *digital evidence interpretation* process and presenting these results in a court of law or to the relevant parties involved. Finally the digital forensic investigation draws to a close within the *investigation closure* process.

Potential digital evidence acquisition process

If this process was not performed during the execution of the acquisitive processes class, this process is performed at this stage. See ‘Potential digital evidence acquisition process’ again for the details in section 3.4.

Digital evidence analysis process

Analysis of the potential digital evidence involves the use of a large number of techniques to identify digital evidence, reconstruct the evidence if needed and interpret it, in order to make hypothesis on how the incident occurred, what its exact characteristics are and who is to be held responsible. Making a hypothesis basically involves the reconstruction of a sequence of events that have led to the current state of the system being investigated. Due to the volume, diversity and complexity of the data to be analyzed in present-day digital forensic investigations, the analysis of evidence becomes a challenge. As volumes of data to be analyzed can be vast, automated techniques are often employed to complement manual analysis techniques. Most of the authors

have split scope of our *analysis process* to several separate processes (6, 9, 11). The authors have decided to propose a single *Analyses* process, whose aim would be to produce hypothesis about incident occurrence and to find appropriate digital evidence to support the hypothesis.

Digital evidence interpretation process

The results from the *digital evidence analysis* process should then be interpreted during this process. Interpretation of any evidence is dependent on the information available about the circumstances surrounding the creation of that item of digital evidence. To be able to carry out a proper interpretation, information from persons involved in the day-to-day running of the system(s) which are being investigated, is often required. Furthermore, information about the purpose of the investigation and a definition of the scope of the investigation is also required. One goal of the *digital evidence interpretation* process is to use scientifically proven methods to explain the facts found during the *digital evidence analysis* process, within the context of the investigation. If the contextual information changes, the interpretation may also have to change to reflect any such contextual information changes. A further goal of the digital evidence interpretation process is to classify the interpreted evidence according to relevance. This means that the evidence, as interpreted, is organized in such a way that it is distinguished which digital evidence artifacts are more important than others. The decision process on deciding which pieces of digital evidence would be more important than others is left to the discretion of one or more competent investigators (2).

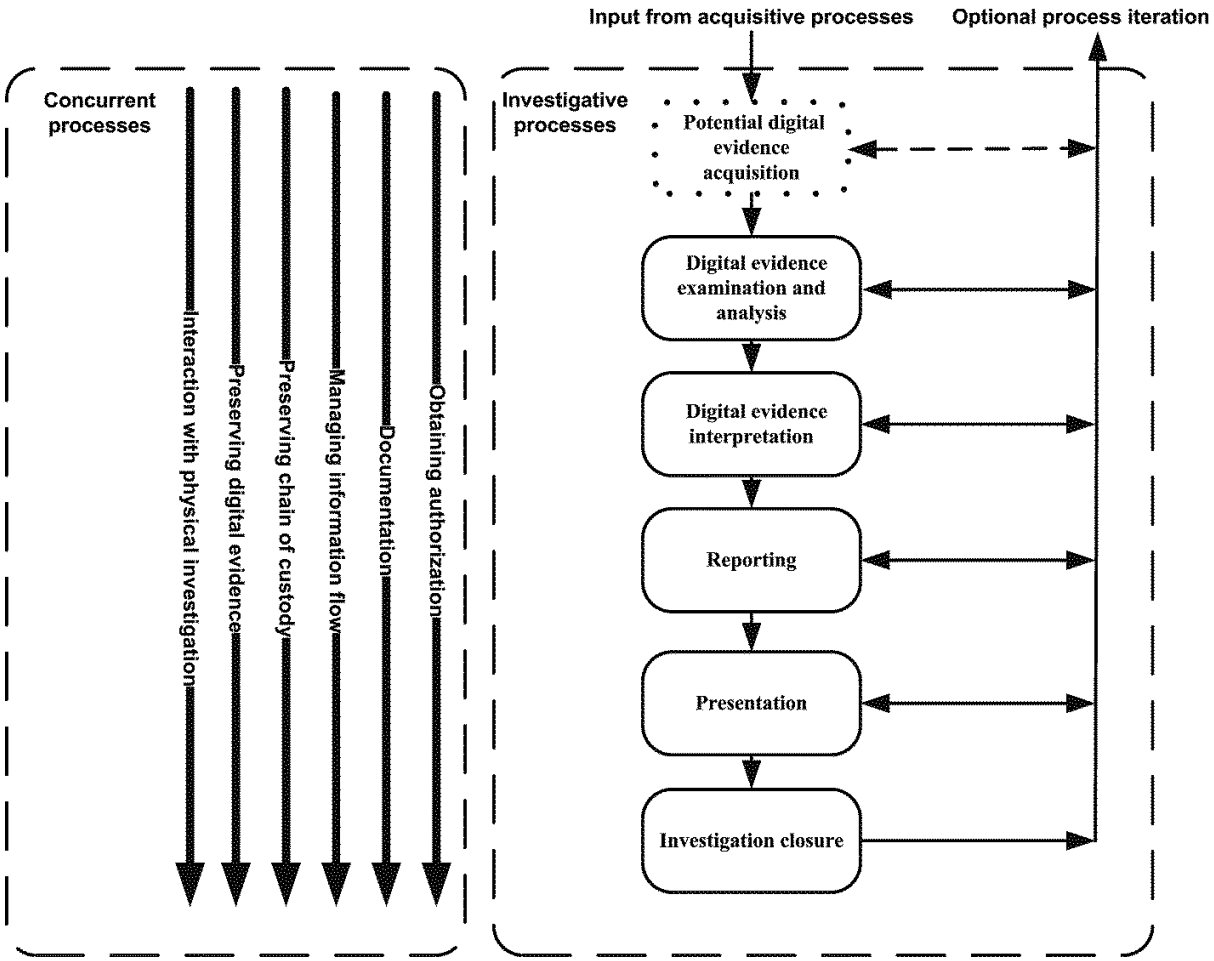

Fig. 6. Investigative processes

Presentation process

The document created during the *report-writing* process is to be presented to all stakeholders. In the case of a court case the stakeholders include the judge, jury, accused, lawyers and prosecutors, as well as any other interested party. In the case of an internal company incident, stakeholders may be the company management team, shareholders and the employees involved. The hypothesis that results from the analysis phase is to be presented together with the identified digital evidence. (Note that not all identified potential digital evidence should be presented – only the relevant identified digital evidence that is of importance for the hypothesis.) The

presentation process also includes proving the validity of the hypothesis if or when the hypothesis is challenged. Thus, the one who presents the hypothesis should be prepared for. Most of the authors have included this as a separate single phase and the authors believe that this is the right interpretation of associated activities.

Investigation closure process

This process concludes the investigation and a decision is to be made on the validity of the hypothesis set in the presentation process. The digital forensic investigation process is iterative. This implies that – after completing this process – one can go back to any of the earlier processes that follow the *first response* process. The closing process should include the following sub-processes: Deciding on need to iterate to a previous process, Acceptance or rejection of the hypothesis, Returning evidence, if needed, Destruction of evidence, if needed. It should be noted that there are various laws in different jurisdictions. The way in which evidence is destroyed, or whether it is destroyed at all, or whether it needs to be stored for a certain period of time after the case has been completed, all depends on the local laws. The investigator should take cognizance of this. Distribution of relevant information to all stakeholders (i.e. communicating the need to iterate to a previous process, deciding on the acceptance or rejection of the hypothesis, or providing any reports or documents from the *presentation* process) should also be performed within this process.

Concurrent processes

Overview of the concurrent processes

In addition to the digital forensic investigation processes, the following processes are also included, which should be considered concurrently with the digital forensic investigation processes: Obtaining authorization (6, 12, 15); Documentation (6, 10-17); Defining the information flow (6, 15); Preserving the chain of custody (1, 6, 10-17) ; Preserving digital evidence (1, 6, 10-17) ; Interaction with the physical investigation (6, 12). Concurrent processes are defined as the principles which should be applied throughout the digital forensic investigation process since such concurrent processes are applicable to many other processes within the digital forensic investigation process. For example, *documentation* is a concurrent process that is applicable to all

processes within the digital forensic investigation process, since all tasks carried out during the entire digital forensic investigation process should be thoroughly logged and documented. The concurrent processes suggested above are justified, since the principles of the digital forensic investigation process, as well as the preservation of the evidence and the chain of custody should be translated into actionable items. These processes should run concurrently with all other processes in order to ensure full admissibility of the digital evidence in a court of law. Moreover, legacy processes (such as *obtaining authorization*, *documentation* and *interaction with the physical investigation*) should actually run across several or all processes. The aim of these concurrent processes is to achieve higher efficiency of the investigation. Information flow should also be defined as a separate concurrent process.

The concurrent processes are explained next.

1. Obtaining authorization

Proper authorization should be obtained for each process performed within all of the digital forensic investigation processes. Authorization might be required from government authorities, system owners, system custodians, principals, users etc. It is important to obtain proper authorization for actions performed during the digital forensic investigation process in order not to infringe on the rights of system owners, custodians, principals or users, but also to ensure that no legal rule is infringed. Needed authorizations would depend on the environment where the digital forensic investigation is performed, both within the legal environment and the organizational environment.

2. Documentation

Each process performed should be documented in order to preserve the chain of custody, but also to improve efficiency and a higher probability of a successful digital forensic investigation. Proper documentation must also be demonstrated during the presentation process.

3. Managing information flow

A defined information flow should exist between each of the processes and among different stakeholders. This information flow has to be defined for each type of investigation. It is important to identify and describe information flows so that they can be secured and supported technologically. For instance, an information flow

could refer to the exchange of digital evidence between two investigators involved in the same investigation. Protection of this information flow can be in the form of, for example, the use of trusted public key infrastructures (PKI) and time stamping to identify the different investigators and authenticate evidence (protecting its integrity), as well as to protect the confidentiality of the evidence through PKI-based encryption.

4. Preserving chain of custody

All legal requirements should be complied with and all processes should be properly documented in order to preserve the chain of custody as the evidence is handled by several parties. This process is to be performed from the *incident detection* process until the last process.

5. Preserving digital evidence

Preserving the evidence means to preserve the integrity of the original digital evidence. In order to achieve this, one must conform to strict procedures from the time that the incident is detected until such time as the investigation is closed. These procedures must ensure that the original evidence is not changed and, even more important, they must guarantee that no opportunity arises during which the original evidence may be changed. This process should also include assessing and documenting the integrity of digital evidence after processing of the evidence. For example, after transporting the evidence or after performing analyses on it, the integrity of the evidence should be confirmed (24).

6. Interaction with physical investigation

Note that the digital forensic investigation process can be dependent on and interconnected with the physical investigation, if such an investigation is conducted in relation to the same incident.

It is often the case that the physical investigation needs assistance from the digital forensic investigation. For example, one such case could be to help determine the movement pattern of the accused via the digital forensic investigation of his mobile phone signal. Another example is the use of digital forensic investigation (of computers, mobile phones, social network activities, email communication, communication via chat rooms and forums etc.) to reveal communication between terror suspects.

On the other hand, the digital forensic investigation might also need assistance from a physical investigation. An example for such a case could be interviewing witnesses (which is an activity within the physical investigation) to supplement results of the digital forensic investigation in the case of an employee stealing intellectual property in the form of copying and using proprietary company information for personal benefit.

Therefore, the proposed *interaction with physical investigation* concurrent process must define the relationship between the digital forensic investigation process and the physical investigation. The interaction is important for preserving the chain of custody, preserving the integrity of the digital evidence, protecting the digital evidence from damage and ensuring an efficient investigation (both for the digital forensic investigation and the physical investigation).

Digital forensic investigation process model schema

Figure 7 represents the entire digital forensic investigation processes, in order to view the digital forensic investigation process in its totality. Note that not all concurrent processes run concurrently with all other processes. For instance, *preserving the chain of custody* and *preserving the evidence interaction* concurrent processes start only with the *implementing pre-incident collection, storage and handling of data representing potential digital evidence* process. However, these are not performed during the *assessment process group* in the *readiness class* of processes. Also, the *interaction with physical investigation* process starts only with the *first response* process.

The digital forensic investigation processes are iterative, which implies that after the last process one can return to previous process. Note, however, that iteration is optional and that one can only return to certain processes, as shown in Figure 7. One can only go back to the following processes: *planning* process, *preparation* process, *incident scene documentation* process, *potential digital evidence identification* process, *digital evidence collection* process, *digital evidence analyses* process, *digital evidence interpretation* process, *report-writing* process or *presentation* process.

The next section discusses the proposed model.

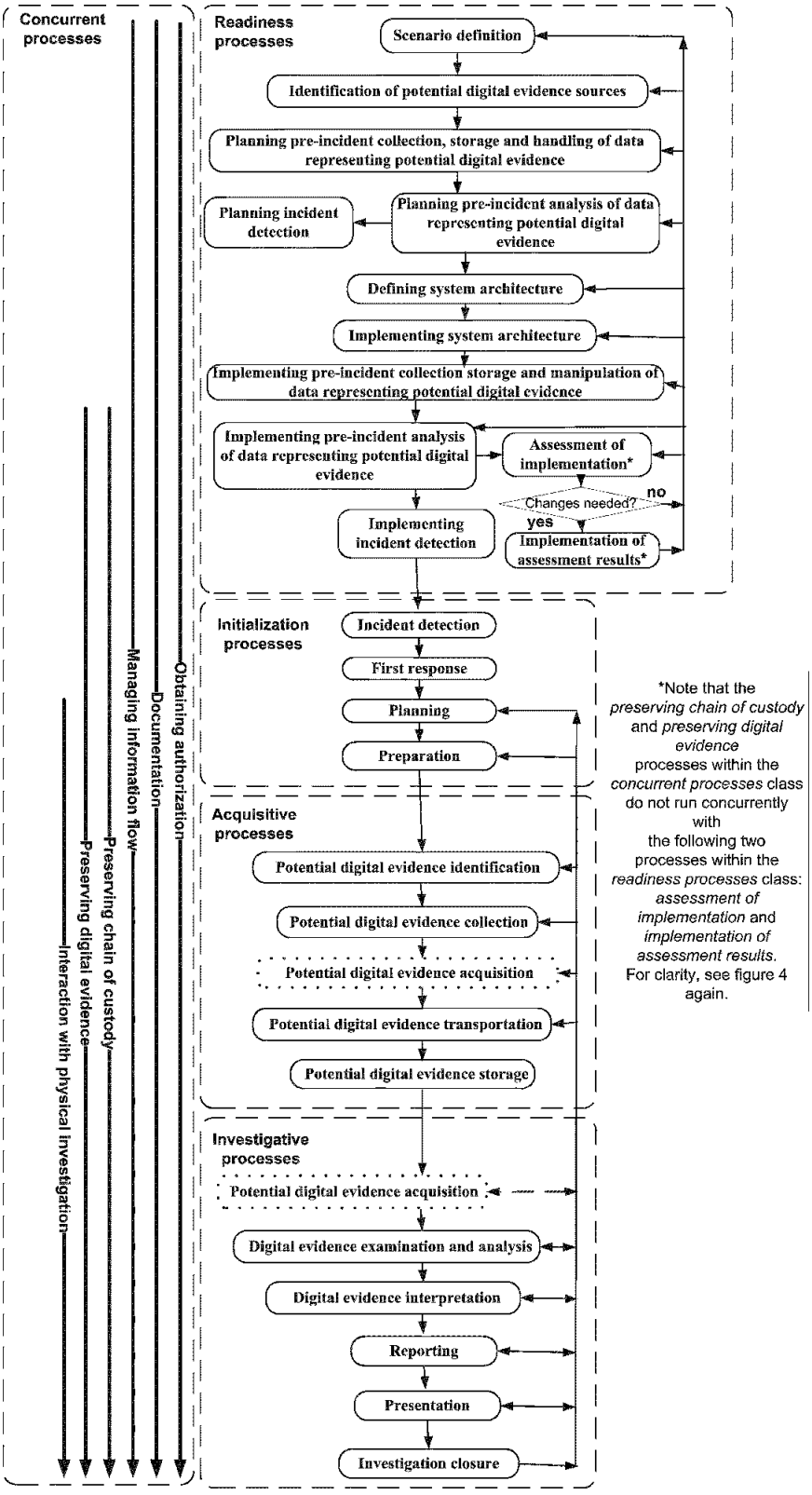

Fig. 7. Comprehensive harmonized digital forensic investigation process

Comparison of existing models to the harmonized model

After defining the harmonized model, the authors have compared it to existing models in order to better explain our model's comprehensiveness. See Appendix A for a table with a detailed comparison. The harmonized process model is mapped to existing models, based on the processes (phases) of each of the models studied.

The harmonized model is iterative and multi-tiered. Sub-processes of the harmonized model are not shown in the comparison table for the sake of simplicity and visual appeal. Each mapped process starts with a number, marking a sequence of processes within the model with which comparison is being made.

Based on the comparison made in Appendix A, the authors claim that the harmonized model is comprehensive. We also introduced the 'concurrent processes' principle, as it would ensure higher efficiency and digital evidence admissibility. This is an important contribution and a novel approach to the principles of digital forensics and will ensure that these principles are consistently applied throughout the digital forensic investigation. Also, the authors have included a comprehensive *readiness processes* class in order to incorporate digital forensic readiness within an organization, before the investigation takes place, if applicable.

Note also that the order of the processes differs from some of the previous models and that the authors believe that the proposed order makes provision for a more efficient investigation process supporting the claims made by the authors in this paper.

Discussion

Our proposed harmonized digital forensic investigation process model is comprehensive and inclusive of all the benefits conveyed by previous models. The processes proposed are well-defined in terms of scope, functions and order. For simplicity of comprehension, the processes have been grouped in process classes. One of the classes is distinctively different from others, i.e. the *readiness processes* class. This class is concerned with

achieving digital forensic investigation readiness for an organization *before* an incident occurs, i.e. it is a proactive approach. The remainder of the process classes, however, follows a reactive approach.

One should note that our harmonized model includes the comprehensive class of readiness processes specifically to ensure that a holistic approach to the digital forensic investigation process is taken and that is a significant contribution of this paper.

In this paper we also proposed several actions to be performed constantly and in parallel with the processes of the model, in order to achieve better efficiency for an investigation and assure the admissibility of digital evidence. We translate these actions to *concurrent processes.* These processes translate the well-established principles in digital forensics. This is a novel approach to the digital forensic investigation process and the authors believe that it can be more functional and effective than existing models. These concurrent processes are an important contribution compared to existing processes and we believe the application of these would enable significantly higher admissibility and efficiency of digital evidence for digital forensic investigations.

The use of the proposed harmonized digital forensic investigation process model could foster many benefits for digital forensic practitioners and academics. Possible benefits include: Higher admissibility of digital evidence in a court of law, due to the fact that a standardized process was used; Human error and omissions during the digital forensic investigation process would be minimized once such a harmonized process was introduced; Usage of the proposed process model across national borders would enable modern society to fight cybercrime far more efficiently, and interaction between private and government entities would also be made much easier and more efficient; The proposed digital forensic investigation process model would enhance the efficiency and effectiveness of digital forensic investigations; Reaching standardization in the field of digital forensic investigation process models.

Conclusion

The problem that this paper addressed is that there is, by the time of writing this paper, no harmonized digital forensic investigation process model that can be used as a standardized set of guidelines for digital forensic investigations. The authors believe that the proposed model is a significant step towards harmonization of existing models. The harmonized model is comprehensive and introduces important novel approaches to the

subject, such as ‘concurrent processes’. The harmonized model aims at enabling efficient and effective digital forensic investigation, and also works towards increasing the admissibility of digital evidence in any court of law. It also aims at achieving digital forensic investigation readiness. The harmonized model should be used by scientists and practitioners in the field in their attempts to adopt the comprehensive harmonized digital forensic investigation process model.

The authors have already started an effort to standardize the process within International Standardization Organization (2). The work presented in this paper is a significant input to the draft standard, ISO/IEC 27043, “Information technology — Security techniques — Investigation principles and processes”, unpublished draft international standard (2). The authors will continue this effort.

Future work should include the development of more procedures to be included as guidelines for the model implementation in respect of different types of digital forensic investigations and different types of digital evidence. Further, future work will be concentrated on evaluating and testing the proposed model and development of a model prototype.

Acknowledgements

Vlatacom Research and Development Center, Milutina Milankovica 5, 11070 Belgrade, Serbia

References

1. Daubert v. Merrell Dow Pharmaceuticals Inc. 509 U.S. 579. (1993).

2. International Organization for Standardization. ISO/IEC 27043; Information technology — Security techniques — Investigation principles and processes. Unpublished final draft international standard. International Organization for Standardization, 2014.

3. Valjarevic A, Venter HS. Harmonized digital forensic investigation process model. Proceedings of Information Security South Africa 2012 Conference; 2012 Aug 15-17; Johannesburg. Johannesburg: Information Security South Africa, 2012.

4. Valjarevic A, Venter HS. Towards a harmonized digital forensic investigation readiness process model. Proceedings of the Ninth Annual IFIP (International Federation for Information Processing) WG 11.9 International Conference. 2013 Jan 28-30. Orlando. IFIP Working Group 11.9 on Digital Forensics, 2013.

5. Pollitt MM. Report on digital evidence. 13th Interpol Forensic Science Symposium. 2001 Oct 16-19. Lyon. Interpol, 2001.

6. Association of Chief Police Officers (ACPO). ACPO good practice guide for computer-based evidence. Association of Chief Police Officers, 2012.

7. Fredesvinda I. The admissibility of electronic evidence in court (A.E.E.C.): fighting against high-tech crime—results of a European study. Journal of Digital Forensic Practice 2006;1:285–289.

8. Mason S. International electronic evidence. London: British Institute of International and Comparative Law, 2008.

9. Palmer G. A road map for digital forensic research, Report from the First Digital Forensic Research Workshop (DFRWS). Digital Forensic Research Workshop (DFRWS); 2001 Nov. 2001. Technical Report DTR-T001-01 FINAL.

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

11. The U.S. Department of Justice. Electronic crime scene investigation- a guide for first responders. The U.S. Department of Justice, 2001.

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

13. Mandia K, Prosise C, Peppe M. Incident response & computer forensics. 2nd ed. Emeryville: McGraw-Hill/Osborne, 2003.

14. Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation 2005;2(2).

15. Ciardhuain SO. An extended model of cybercrime investigations. International Journal of Digital Evidence 2004;3(1).

16. Casey E, Rose CW, Forensic Analysis. In Casey E, editor. Handbook of Digital Forensics and Investigation. Elsevier Science, 2009.

17. Cohen FB. Fundamentals of digital forensic evidence. In Stavroulakis P, Stamp M. Handbook of information and communication security. Springer, 2011;789-808.

18. Carrier B, Spafford EH. An event-based digital forensic investigation framework. Digital Investigation 2005;2(2).

19. Cohen FB, Lowrie J, Preston C. The state of the science of digital evidence examination. http://www.all.net/ForensicsPapers/2011-01-30-IFIP-Accepted.pdf, 2011.

20. Tan J. Forensic readiness. Cambridge USA: @stake Inc., 2001.

21. Yasinsac A, Manzano Y. Policies to enhance computer and network forensics. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. 2001 Jun 5-6. West Point. IEEE, 2001.

22. Wolfe-Wilson J, Wolfe HB. Management strategies for implementing forensic security measures. Information Security Technical Report 2003;8(2):55-64.

23. Rowlingson R. A ten step process for forensic readiness. International Journal of Digital Evidence 2004;2(3).

24. Casey E, Schatz B. Conducting Digital Investigations. In Case E, editor. Digital evidence & computer crime. 3rd ed. Elsevier Science, 2011;187-227.

Additional Information and Reprint Requests

Mr. Aleksandar Valjarevic

Mailing address: PO BOX 4897, Rivonia, 2128, South Africa

Appendix A- Table 1: Comparison of existing models to the proposed harmonized model

	The harmonised model	Palmer [9]	Reith et al. [10]	DOJ [11]	Carrier and Spafford [18]	Mandia et al. [13]	Beebe and Clark [14]	Cuardhuain [15]	Cohen [17]	Casey and Rose [16]	ACPO [6]
	Processes										
1.	Incident detection	1. Identification	1. Identification		2. Detection and notification	2. Detection of the incident 3. Initial response	2. Incident response	1. Awareness			
2.	First response					3. Initial response	2. Incident response				2.1 Secure and control the crime scene
3.	Planning		3. Approach strategy		1. Readiness group of processes	4. Response strategy formulation		3. Planning			1. Preparations for investigation
4.	Preparation		2. Preparation	1. Preparation	1. Readiness group of processes	1. Pre-incident preparation	1. Preparation				1. Preparations for investigation
5.	Incident scene documentation			3. Documentation of the crime scene	4.3 Document evidence and scene						2.1 Photograph and document the scene 2.4 Attaching exibit labeles
6.	Potential digital evidence identification		6. Examination	2. Recognition and Identification;	4.2 Survey for digital evidence			5. Search for and identify evidence	1. Identification	1.Gather information and make observations,	5.1 The collection process
7.	Digital evidence collection	2. Preservation 3. Collection	4. Preservation 5. Collection	4. Collection and preservation	4.1 Preservation of digital crime scene	5. Duplication 7. Secure measure implementation 8. Network monitoring	3. Data collection	6. Collection of evidence	2. Collection 3. Preservation	1.Gather information and make observations,	2.3 Initial collecting of volatile data 5.1 The collection process
8.	Digital evidence transportation			5. Packaging and transportation				7. Transport of evidence	4. Transportation		3. Transport
9.	Evidence storage							8. Storage of evidence	5. Storage		4. Storage
10.	Digital evidence analysis	4. Examination 5. Analysis	7. Analysis	6. Examination 7. Analysis	4.4 Search for digital evidence	6. Investigation	4. Data analysis	9. Examination of evidence	6. Analysis		5.2 The analysis process
11.	Digital evidence interpretation				4.5 Digital crime scene reconstruction			10. Hypothesis	7. Interpretation 8. Attribution 9. Reconstruction	2. Form hypothesis to explain observa-tions, 3.Evaluate the hypothesis, 4. Draw conclu-sions and commu-nicate findings.	5.3 The examination process
12.	Report-writing			8. Report		10. Reporting					5.4 The reporting process
13.	Presentation	6. Presentation	8. Presentation	8. Report	4.6 Presentation of digital scene theory	10. Reporting	5. Findings presentation	11. Presentation of hypothesis 12. Proof/Defence of hypothesis	10. Presentation	4 .Draw conclusions and communicate findings.	5.4 The reporting process
14.	Investigation closure	7. Decision	9. Returning evidence			9. Recovery 11. Follow-up	6. Closure	13. Dissemination of information	11. Destruction		6. Disclosure
	Concurrent Processes										
1.	Interaction with physical investigation				† (3. Physical crime scene investigation group of phases)						Present as principle and set of processes, including preservation of physical evidence and interviews
2.	Preserving chain of custody	*	*	*	*	*	*	*	*	*	*
3.	Preserving digital evidence	*	*	*	*	*	*	*	*	*	*
4.	Information flow							Described			Partially described
5.	Documentation	*	*	*	*	*	*	*	*	*	*
6.	Obtaining authorization				† (2.Confirmation and authorization process)			† (2. Authorization)			*

Appendix A- Table 1: Comparison of existing models to the proposed harmonized model

Key:

* Present as principle

† Present as process (description of a specific process that relates to a specific digital forensic principle)