Introduction of Concurrent Processes into the Digital Forensic Investigation Process

Aleksandar Valjarevic[1](corresponding author),
[1]*Department of Computer Science, University of Pretoria, Pretoria, South Africa*
Postal address: P.O. Box 4897, Rivonia, 2128, South Africa
Tel:+27 78 250 84 35
Fax:+27 86 239 6207
Email: alexander@vlatacom.com

Hein S. Venter[1],
[1]*Department of Computer Science, University of Pretoria, Pretoria, South Africa*
Postal address: Office: 4-23, Department of Computer Science, IT Building, University of Pretoria, Lynnwood Drive, Pretoria, 0002, South Africa
Tel:+27 83 458 4407
Fax:+27 86 239 6207
Email: hventer@cs.up.ac.za

Abstract— Performing a digital forensic investigation requires a formalized process to be followed. It also requires that certain principles are applied, such as preserving of digital evidence and documenting actions. The need for a harmonized and standardized digital forensic investigation process has been recognized in the digital forensics community and much scientific work has been undertaken to produce digital forensic investigation process models, albeit with many disparities within the different models. The problem is that these existing models do not include any processes dealing explicitly with concurrent digital forensic principles. This leaves room for human error and omissions, as there is a lack of clear guidelines on the implementation of digital forensic principles. This paper proposes the introduction of concurrent processes into the digital forensic investigation process model. The authors define concurrent processes as the actions which should be conducted in parallel with other processes within the digital forensic investigation process, with the aim to fulfill digital forensic investigation principles. The concept of concurrent processes is a novel contribution that aims to enable more efficient and effective digital forensic investigations, while reducing the risk of human error and omissions which result in digital evidence being contaminated.

***Keywords*— concurrent processes, digital forensic process, harmonized digital forensic investigation process, digital forensic principles**

1. INTRODUCTION

Digital forensics has gained significant importance over the past number of years. Information security incidents are constantly on the rise and highlight the importance of digital forensic investigation abilities. The fact that society depends heavily on information technology also contributes to the importance of digital forensics.

Dealing with digital evidence requires a standardized and formalized process to be followed in order for digital evidence to be accepted in a court of law. Without the intent to advocate a specific legal system, consider the following example. In the United Stated of America cases that require the presentation of digital evidence are treated under rule 702 of the Federal Rules of Evidence [1], which says: "If scientific, technical, or other specialised 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." The Daubert ruling [2], which is used in the US for expert witness testimony in digital forensic investigation cases is important for the application of the above mentioned rule [1]. Part of the Daubert ruling [2] states that theories and techniques used to draw conclusions in a digital forensic case must result in positive answers to a number of questions, notably the question of whether the theories and techniques used during a digital forensic investigation are subject to standards governing their application. Other countries have similar guidelines aimed at digital forensic investigations or parts of it [3, 4, 5]. All of the above clearly indicates the need for one harmonised and standardised digital forensic process to be followed when performing digital forensic investigations.

In the past decade, a number of academic research projects were conducted in order to establish a digital forensic investigation process model. The existing digital forensic process models vary in structure, number and type of process. All the process models include digital forensic principles that must be followed when performing a digital forensic investigation. Digital forensic principles can be defined as general rules and requirements in regard to the digital forensic investigation process. These rules and requirements ensure that investigation results are valid, that the integrity of the digital evidence is preserved and that it the digital evidence is acceptable to the relevant authorities, such as courts or any other authority that is being presented with digital evidence. These principles are applicable to any type of digital forensic investigation.

Digital forensic principles most often described in literature include preserving digital evidence, preserving chain of custody and documenting actions. However, often existing models provide neither clear guidelines nor processes to be followed in order

for these principles to be applied. Further, there exist disparities on when these principles need to be applied and on the duration of actions implementing the principles.

The authors define the problem to be addressed in this paper as follows: existing digital forensic investigation process models do not include any processes relating to the application of digital forensic principles that stretch across the duration of a digital forensic investigation (such as preserving evidence, preserving chain of custody or documenting actions).

Some of the existing models, such as Palmer [6], Reith et al. [7] and Carrier and Spafford [8] do include such processes, but they are not defined to run concurrently with other investigation processes; instead they are very limited in time and often presented as a single, sequential process, hence not ensuring the adherence to the principles over the complete course of the investigation. This creates the possibility of errors and omissions when implementing digital forensic principles and also possible risk for the investigation (for example, the risk of compromising digital evidence).

The authors propose the introduction of concurrent processes to address the problem. The introduction of concurrent processes can be illustrated by the following example.

Suppose obtaining authorization takes place as only one process within the model, limited in time; this means that a request for authorization for certain actions will only take place at one stage of the investigation. This is not practical, as different authorizations might be needed during the course of the investigation. For example, the following authorizations are often needed during an investigation: authorization by information system owners and custodians to perform potential digital evidence collection; authorization by an information system user if private information is collected; authorization from a state authority, if required, to perform an investigation; authorization by a system owner to present investigation findings to stakeholders; authorization to dispose of digital evidence; etc. The introduction of concurrent processes would enable higher admissibility of digital evidence and more efficient investigations. The reason is that the introduction of the proposed processes would ensure that digital forensic principles are correctly applied throughout the course of the digital forensic investigation, thus ensuring the acceptability of digital evidence and investigation results. Further, investigations could be more efficient, as one could plan in advance for the implementation of the proposed processes that ensure the correct application of the digital forensic principles. Also, some of the proposed processes are prerequisites for efficient digital forensic investigation and if omitted can create delays and problems. Examples of this are interaction with the physical investigation and obtaining appropriate authorization for actions.

The introduction set the scene and stated the problem to be addressed. The remainder of the paper is structured as follows. Section II provides background on digital forensics and presents related work in regards to digital forensic investigation process models. After that, Section III presents proposed concurrent processes to be incorporated in the digital forensic investigation process, with the aim to increase effectiveness of digital forensic investigations and also increase admissibility of digital evidence. Testing and evaluation of implementing the proposed concurrent processes is described in Section IV. Testing was performed on real world cases. Testing was qualitative and the paper presents findings in regards to benefits of implementation of the proposed concurrent processes. Section V concentrates on discussing the proposed concurrent processes, contribution to the field and potential benefits. Last section, Section VI, concludes this paper and provides indications of future work.

2. BACKGROUND

The subsections to follow provide background on the following topics. First, background on digital forensics is provided to introduce the reader to the basic definition of digital forensics. After that, we provide background on the legal aspects of the digital forensic investigation processes that provides a motivation for the use of formalized and standardized processes.

A. On Digital Forensics

In this section the authors provide a definition of digital forensics compiled from various sources used in 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 [9].

B. Related Work on Digital Forensic Investigation Process Models

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 [6], the need for a standard framework for digital forensics has been widely acknowledged [7,8, 10, 11, 12, 13, 14].

What follows is an overview of the existing digital forensic investigation process models.

- Reith et al. [7] propose a digital forensic investigation process model known as the abstract model.
- The U.S. Department of Justice (DOJ) published a process model in the Electronic Crime Scene Investigation Guide aimed at first responders [15].
- The model proposed by Carrier and Spafford [8] is based on physical crime investigation.
- Carrier and Spafford also propose another (similar) event-based process model [16].

- Mandia et al. propose a digital forensic investigation process known as the incident model [15].
- Beebe and Clark propose a hierarchical, objectives-based digital forensic investigation process [12].
- Cuardhuáin [11] proposes an extended and comprehensive model of cybercrime investigations. The harmonized model also includes a description of information flow between different processes. Cohen [18] proposes a process model that includes the following processes: identification, collection, preservation, transportation, storage, analysis, interpretation, attribution, reconstruction, presentation and destruction.
- Casey and Rose [13] define processes of the digital forensic investigation process as: gather information and make observations, form a hypothesis to explain observations, evaluate the hypothesis, draw conclusions and communicate findings.
- In the United Kingdom examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and integrity of evidence [17].

The following digital forensic principles were identified by the authors of this paper in the models that were analyzed during this research:

(1) Obtaining authorization [8,11,17]
(2) *Documentation* [7,10,11,13,15,17,18]
(3) Information flow [11, 17]
(4) *Preserving chain of custody* [7,10-13,15,17,18]
(5) *Preserving digital evidence* [7,10-13,15,17,18]
(6) Interaction with physical investigation [8,17]

Table 1 provides a summary of digital forensic principles included in the models that were analyzed during this research. Note that some of the models only include principles, while others have descriptions of activities that must be performed to apply the principles, and some even translate principles into processes or sets of processes.

Table1: Overview of digital forensic principles within state-of-the art digital forensic investigation process models

		Palmer [6]	**Reith et al.[7]**	**Carrier and Spafford [8]**	**Mandia et al. [10]**	**Cuardhuáin [11]**	**Beebe and Clark [12]**	**Casey and Rose [13]**	**DOJ [15]**	**ACPO [17]**	**Cohen [18]**
Digital forensic principles											
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)				*	

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

Based on related work, the authors 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, 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 physical crime investigation processes).

With regard to digital forensic principles and their incorporation in the existing models, the authors conclude the following:

(1) Three of the principles detected in the analyzed models (preserving chain of custody, preserving digital evidence and documentation) are present – only as principles – in all of the analyzed models.

(2) The other three of the principles identified (interaction with the physical investigation, managing information flow and obtaining authorization) are present in only three of the analyzed models. In addition, they have been introduced in disparate ways, i.e. either as principles, as a description of activities or as processes within the model.

Disparities that were identified in the existing models show that there is a low level of harmonization in regards to digital forensic principles and its application. This can lead to consequences, especially in cases of cross-border and cross-jurisdiction digital forensic investigations. Consequences can include, but are not limited to the following:

- Legal and procedural issues and errors can occur if proper authorizations are not in place for each action within the investigation. For example, when performing internal digital forensic investigation on behalf of a company, one must ensure that the company's legal representative or authorized person gives authorization for any action taken on the company's information systems. Potentially, system users might also need to give authorization if their personal data is being accessed. If this is not observed, it can lead to violation of the company's policies or even applicable laws, such as privacy law.
- Issues with evidence integrity and process integrity can occur if documentation is not performed properly for each action within the investigation. For example, if examination, analysis and interpretation of digital evidence are not properly documented, the results of digital forensic investigations can be questioned.
- Issues with efficiency, effectiveness and privacy-related issues can occur if information flow is not defined. As in every activity where multiple persons and entities are involved it is of crucial importance for the efficiency and effectiveness of the digital forensic investigation, to have defined information flows as well as functional information flows, which will promote collaboration and information sharing. Also, this should prevent dissemination of information to unauthorized users and preserving confidentiality and integrity of such information.
- Integrity and admissibility of digital evidence can be questioned if processes of preserving digital evidence and preserving the chain of evidence are not implemented throughout the investigation. If at any step of the investigation these are not strictly implemented, digital evidence and conclusions of the investigation might be in question.
- Potential digital evidence may be lost or corrupted if proper coordination with the physical investigation does not exist. If the physical investigation of the crime scene takes place before the digital forensic investigation, the digital evidence can be lost or corrupted. For example, this would happen in case investigators performing a physical investigation switch off computers, thus preventing any potential live forensic investigation.
- Errors and omissions can occur when implementing any of the principles as there exist no harmonized and internationally-accepted guidelines on implementation of these principles.

Considering the above, it is clear that harmonization is required for digital forensic principles and also for ways these should be applied within the digital forensic investigation process model. For the purpose of this paper, harmonization can be defined as adjustment of differences and inconsistencies among different processes to make them uniform, mutually compatible and more effective. This is a modified definition presented in the Business Dictionary [19], for the purpose of this paper and the subject.

The following section presents the proposed introduction of concurrent digital forensic investigation processes.

3. INTRODUCTION OF CONCURRENT PROCESSES

This section describes the proposed introduction of concurrent processes. The concurrent digital investigation processes are described in this paper at such a level of abstraction so that they can be used for different types of digital forensic investigation and for different types of digital evidence.

For example, the proposed concurrent processes could be used for a digital forensic investigation on a standalone computer, on a mobile device, in a networked environment or even in a cloud-computing environment. In addition, the model can be used for different types of digital evidence, such as data on a hard drive or solid state drive; volatile data (such as RAM memory); and live data such as network traffic data.

The authors introduce a novel approach in the way some of the digital forensic principles have been applied, namely *concurrent processes*. The authors define concurrent processes as the principal actions that should be achieved in parallel with other processes within the digital forensic investigation process (e.g. the principal action that ensures the documentation of all actions throughout the entire investigation process takes place).

The authors believe that the introduction of a class for concurrent processes is a significant contribution, which would enable more efficient and reliable investigations as well as promote stricter adherence to the investigation principles of digital forensics.

As explained in the introductory section of this paper, the significant contribution lies in the fact that the introduction of the proposed concurrent processes would ensure that digital forensic principles are correctly applied throughout the course of digital

forensic investigations. Also, the introduction of the proposed concurrent processes would enable planning of their implementation in order to make the investigation more efficient. Finally, in our opinion, some of the proposed processes are prerequisites for efficient digital forensic investigations and, if omitted, can create serious investigation delays and implementation issues. Examples of such proposed processes include interaction with the physical investigation scene and obtaining appropriate authorization for actions carried out during the investigation. If these are not well planned and executed, a digital forensic investigation might not be efficient and digital evidence might be at risk of being contaminated. Further, an investigator could document only the crime scene, but omit to document each and every action within the digital forensic investigation process. It is especially important that throughout the investigation, principles of preserving digital evidence and preserving the chain of custody should be implemented concurrently, as any minor omission here can contaminate digital evidence and make it unusable in court of law.

For illustration purposes only, the authors' previous work [20] and international standard ISO/IEC 27043:2015 [9] (to which the authors have contributed significantly) are used to show how the concurrent process are applied to the rest of the digital forensic investigation process. The authors do not aim in this paper to propose or describe in detail the other processes within the harmonized process model, except for the concurrent processes. The other processes will, however, be very briefly described for illustrative purposes.

In order to abstract all processes on a higher conceptual level, all digital forensic investigation processes can be categorized into the following digital forensic investigation process classes [9]: readiness processes class, initialization processes class, acquisitive processes class, investigative processes class and concurrent processes class.

These classes are discussed in the following subsection. The authors present this overview in order for the reader to gain a holistic view of the digital forensic investigation process model. In addition, one should also then be able to understand the basics of each of the classes, as well as how these classes relate to one another, before examining the details of the concurrent processes class and their relation to the other subprocesses.

A. ***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: readiness, initialization, acquisitive, investigation, and concurrent.

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 process should also enable preserving or improving the information security of potential digital evidence, i.e. securing the data in terms of its confidentiality, integrity and availability (CIA). Note that the readiness processes are optional to the rest of the digital forensic investigation processes. The main reason for this is that the readiness processes are carried out in a proactive manner compared to the rest of the investigation processes, which are reactive in nature. In addition, the implementation of the readiness processes depends on the budget and discretion of the information system owner/custodian.

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 and planning and preparation of the actual digital forensic investigation. These processes are of extreme importance to the success and effectiveness of the investigation.

The acquisitive class of processes deals with the investigation of the physical scene of a case. Processes in this class are concerned with acquisition of digital evidence and include incident scene documentation, digital evidence identification, collection, transportation and storage of digital evidence. These processes are very important and are crucial for the digital forensic investigation, and the validity and relevance of digital evidence depend heavily on these processes.

The investigative class of processes deals with uncovering the digital evidence. This class has the aim of producing a hypothesis about the events that resulted in the need for an investigation. It analyzes and interprets digital evidence acquired in order to relate it to actual events and entities (i.e. people and computers). Processes in this class are concerned with digital evidence analyses and interpretation, followed by reporting, presentation and investigation closure.

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 the forensic principles are implemented and followed, ensuring the admissibility of proper digital evidence and digital investigation effectiveness. Translating these principles into actionable items makes it easier for practitioners to strictly adhere to them.

Figure 1 shows the classes of digital forensic investigation processes and an overview of their relationships. As shown in Figure 1, the *concurrent processes* class runs in parallel with all other classes, ensuring greater digital forensic principles.

The following subsections provide details on each of the processes within the proposed concurrent process class.

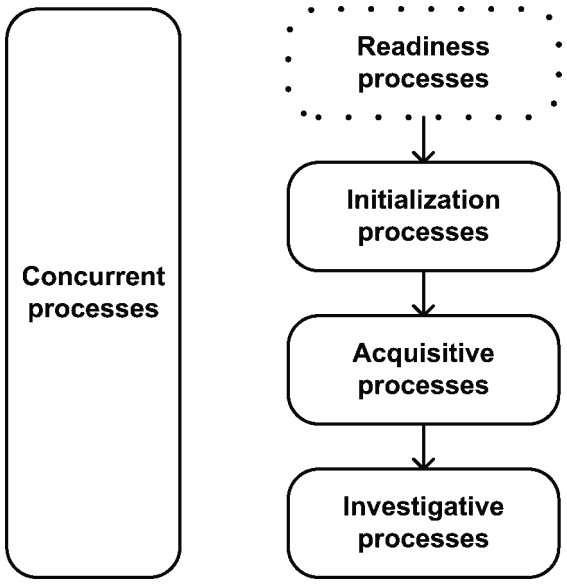

Figure 1. The classes of the comprehensive harmonized digital forensic investigation process model

B. ***Concurrent processes***

1) Overview of the concurrent processes

Concurrent processes are defined as the principles that should be applied throughout the digital forensic investigation process, since such concurrent processes are applicable to many other processes within a digital forensic investigation. 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 following processes are included in the digital forensic investigation process model as concurrent processes: obtaining authorization, documentation, information flow, preserving chain of custody, preserving digital evidence, and interaction with the physical investigation.

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 that the digital evidence is admissible 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 concurrent processes are explained next.

2) 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. The specific authorizations needed would depend on the environment (both legal and organizational) in which the digital forensic investigation is performed.

3) Documentation

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

4) 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 done by, for example, using trusted public key infrastructures (PKI) and time stamping to identify the different investigators and authenticate evidence (protecting its integrity). PKI-based encryption can also protect the confidentiality of the evidence.

5) Preserving the 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.

6) 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 it is processed. For example, if the evidence has been transported or if analyses have been performed on it, the integrity of the evidence should be confirmed [21].

7) Interaction with physical investigation

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. Therefore, this activity 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.

*C. **Digital forensic investigation process model schema***

Figure 2 represents a summary of the entire digital forensic investigation process. It shows the relation of the concurrent processes to the processes from the other classes. Note how not all concurrent processes run concurrently with all of the other processes. For instance, *preserving chain of custody*, *preserving digital evidence* and *interaction with physical investigation* concurrent processes start only with the initialization processes class, because it is only within this class that one starts dealing with digital evidence and might also interact with physical evidence and the physical investigation process.

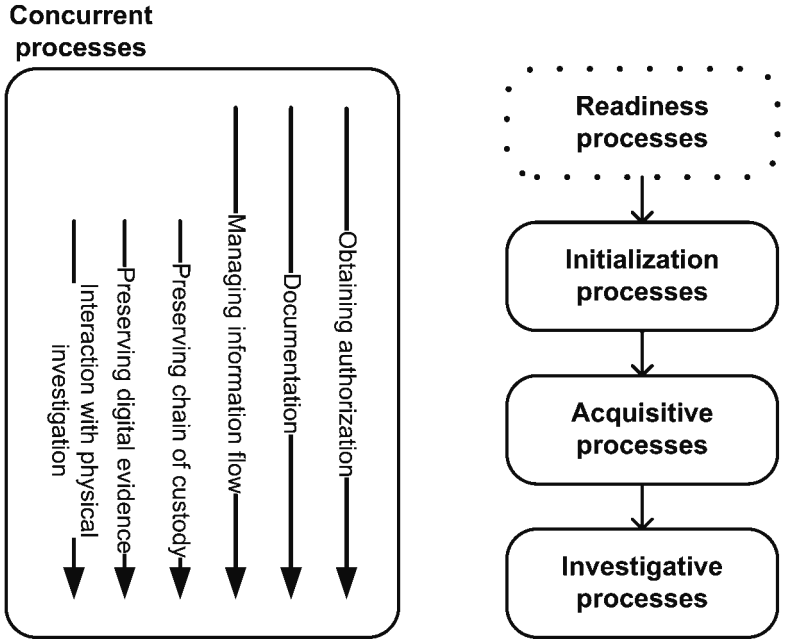

Figure 2. Summary of the digital forensic investigation process schema

4. TESTING

In this section the authors analyse results of implementation of the proposed concurrent processes to real-world test cases in order to evaluate usability and effectiveness of the proposed process model.

Testing was performed by the authors and fellow researchers from ICSA (Information and Computer Security Architecture) research group of the Computer Science Department of the University of Pretoria. Further, the conclusions of this testing were published in relevant papers [22,24,25]. In order to complete this task there was collaboration with a digital forensic investigations private company (who will remain anonymous), who provided their equipment, software and expert advice needed to perform digital forensic investigations.

Evaluation was performed based on the following evaluation parameters:

1. **Could the proposed processes accommodate all needed activities and processes within the digital forensic investigation for a specific case and specific type of the digital forensic investigation?**
   This parameter shows whether the processes were applicable to specific case and specific type of digital forensic investigation. If the parameter is met for different types of digital forensic investigations and different cases it would mean that the proposed processes are general enough to be applied to broad field of digital forensic investigations. Similar requirement for digital forensic process models was set by Carrier and Spafford [8].

2. **Did the proposed processes assist the investigators to improve admissibility of digital evidence?**
   This parameter shows if the proposed processes contribute to improving admissibility of digital evidence, through providing concrete means to assist preserving evidence integrity. Achieving admissibility of digital evidence and preserving integrity of digital evidence is one of main aims of digital forensic investigations as identified by many authors in the field [7, 15, 18].
3. **Did the proposed processes assist with effective and efficient collaboration within the digital forensic investigation for a specific case?**
   This parameter shows if the proposed processes assist with and promote collaboration of different investigators or event different organizations when performing digital forensic investigation. Collaboration is becoming more and more important aspect of digital forensic investigations in the light of growing amount of data needed to be analyzed within investigation and in the light of growing number of cross-jurisdiction and cross-border investigations. This fact was recently recognised and emphasised in the 2014 Internet Organised Crime Threat Assessment (iOCTA) document [26] prepared by European Cybercrime Centre at Europol.
4. **Did the proposed processes improve on expected efficiency and effectiveness of the digital forensic investigation?**
   This parameter shows if the proposed processes can help with achieving higher efficiency and effectiveness of the digital forensic investigation. In practice this would mean maximizing success rate of investigation, whilst minimising the costs of an investigation. This requirement appears prominently in related work, and especially in work concentrating on digital forensic readiness [27].

Parameters are qualitative and investigators expert opinion was used to determine whether during the implementation of the proposed processes on a specific case the above parameters were met.

Each of the three cases is discussed in more detail in the sections to follow and the structure of each discussion is as follows: For each of the presented cases, the testing methodology is explained first. Next the case scenario is presented, followed by findings and observations.

Note that the authors do not intend to present the detailed overview of each action taken within this investigations nor the full results of the investigations, as that would be out of the scope of the paper.

A. Case 1-Mobile digital forensic investigation in regards to phishing using a scareware attack [22]

The testing was carried out with commercial mobile forensics software of the Micro Systemation (MSAB) XRY V6.5 Mobile Forensic toolkit [23].

In the *preparation* process, the following equipment was needed [22]: the XRY complete toolkit for mobile device examinations; an XRY licence key USB stick; a write blocker; a forensically cleaned USB drive; a desktop PC with Windows OS 8; a SIM adapter; a forensically cleaned hard drive; and an empty DVD. A Faraday bag was used to package and isolate the mobile device from the network during a *potential digital evidence collection* process, while a digital camera was used to document the potential evidence and crime scene.

The proposed process model was tested through its implementation in a real-world case involving a mobile device with an Android operating system. Due to the confidentiality agreements in place and the sensitivity of the case, some of the details presented in the case scenario are withheld or rendered anonymous.

The case analyzed is a phishing attack using scareware, targeted at bank X customers via short message services (SMS). The mobile device targeted with the SMS scareware is a Samsung mobile Galaxy S2 phone belonging to customer X of bank X. The suspect/attacker distributes scareware to bank X clients via a SMS. The suspect/attacker sent scareware SMSs to the clients, mimicking Bank X by requesting the clients to click on the sent link to update their account details or else lose their data held with the bank. The unsuspecting bank X customer fell victim to such a phishing attack. The suspect further performed an unauthorized transaction on the customer's bank account as a result of the customer's details that were collected. A transaction alert received by the bank's customer that he/she never initiated, raised the customer's suspicion. The customer then reported the incident to bank X.

The case was successfully resolved and the perpetrator was identified and charged. The findings and observations are as follows [22]:

- A valuable contribution is the introduction of the concurrent processes, which helped preserving the integrity of the investigation and digital evidence. Omeleze and Venter [22] identified documentation as a single most important process among concurrent processes and have concluded that this process enables coherence between other concurrent processes. It was also concluded that the documentation process is essential in maintaining information flow and ensuring that the chain of custody is adequately observed. If concurrent processes are not closely followed there is a greater chance of potential evidence contamination, rendering a case inconclusive or invalid when presented to stakeholders.
- The proposed process model accommodates [22] the investigation of Android devices, and therefore it can be reasonably assumed that it accommodates investigation of mobile devices in general, effectively, as long as the concurrent processes are strictly implemented from the beginning of an investigation to its conclusion.

B. Case 2- Mobile digital forensic investigation in regards to the stealing of intellectual property [24]

Testing methodology was the same as for the previous case described. The case included mobile forensic activities for a Blackberry mobile device as will be explained below.

In this case study, Company X holds intellectual property rights for the advertising concepts developed by their creative team. Non-compete agreements are in place to deter an employee from stealing intellectual property from an employer and creating a competing entity using the former employer's intellectual property.

The investigation was successful and the results obtained from the interpretation process of the investigation showed that the former employee of Company X used the mobile device for stealing intellectual property with the aim to create a competing entity. Company X received all necessary reports and information during investigation closure process, after which they could use these to prosecute the perpetrator.

The findings and observations are as follows [24]:

- The documentation concurrent process has proved to be vital during the testing in order to insure adherence to digital forensic principles. Implementation of concurrent processes ensures that the person conducting the investigation activities performs actions needed to ensure digital forensic principles are adhered, which, in turn, ensures higher admissibility of digital evidence and higher admissibility of findings and results of an investigation.
- The concurrent processes were applied throughout the testing. It was concluded that the proposed concurrent processes are fully applicable to mobile digital forensic investigations, thus, showing its adaptability to different types of digital forensic investigations.

C. Case 3- Digital forensic post mortem investigation in regards to contravention on company user policy [25]

During the *preparation* process, the investigators prepared all relevant equipment and resources as will be described in Table 6.2 [25].

Table 2 List of resources and equipment prepared for the investigation [25]

Resources (Item)	Purpose of the Resources
Two forensically clean drives	Used as a destination to store the imaged hard disk for processing. The second drive is a backup used to store the copy of the imaged hard disk, in case the destination drive is corrupted or compromised.
Tableau TD2 forensic duplicator (2013)	Used for imaging the hard disk without compromising it.
Hardware-based write blocker device	Used to ensure that Windows does not alter the suspect's hard disk when attached to the computer.
A blank DVD	Used to provide a copy of the potential digital evidence obtained during the investigation.
A digital camera	Used to take photographic images of the evidence and crime scene.
A Faraday bag	Used to package potential digital evidence during the digital evidence collection process.
A USB Dongle	Plugged into the investigator's computer to run Access Data FTK in full mode.
Forensic Toolkit (FTK) 3.2 imager	Used to preview recoverable data from a disk, as well as to create perfect copies, called forensic images.
Software products keys	Used to ensure that the software application is genuine.

The scenario used was as follows: Company X suspected one of their employees of using company resources to download pornographic material during office hours. Company X regards any form of pornography as illegal and unacceptable, according to their user policy.

The investigation was successful. The results obtained from the interpretation process showed that the employee of Company X had violated company policy with regard to internet usage. The digital evidence found included photos, documents and videos. Based on reports and information handed to Company X, Company X proceeded to make a decision on the case based on the company's policy.

The findings and observations are as follows [25]:

- The concurrent processes were adequately adaptable during the post mortem digital forensic investigation. It was concluded that the proposed concurrent processes are fully applicable to post-mortem digital forensic investigations. We have already seen that the proposed concurrent processes are applicable to mobile digital forensic investigations and, combined with this conclusion, we can comfortably say that the proposed concurrent processes are adaptable. The

concurrent processes assisted in the preservation of integrity, confidentiality and availability of the potential evidence. It was noted [25] that the concurrent processes ensured that each step conducted during the investigation was documented and each interaction was accounted for by clearly adhering to the rules and norms of conducting a forensically sound investigation. Consequently we can say that the implementation of concurrent processes enables an investigator to achieve higher admissibility of digital evidence, findings and results of the investigation. Further it helps the investigator to more easily follow the course of the investigation.

D. Summary of testing results

Based on tests performed on real world cases as described in sections above, it can be concluded that the concurrent processes proposed can be implemented for different types of digital forensic investigations, such as mobile forensic and post-mortem forensic cases, thanks to their adaptability.

Further implementation of these processes helps following proper legal processes and procedure, preserving integrity of the investigation and digital evidence.

Ultimately, it can be concluded that the proposed concurrent processes do enable one to effectively follow a proper digital forensic investigation process and increase the admissibility of digital evidence. This should also increase the admissibility of the results and findings of the digital forensic investigation at hand.

Revisit the evaluation parameters defined above in order to see what conclusions can be drawn from the presented cases. The following table summarizes conclusions for the three cases in regards to defined evaluation parameters.

Table 3 Evaluation parameters

Evaluation parameters	Case 1 (mobile- Android)	Case 2 (mobile-Blackberry)	Case 3 (post-mortem)
Could the proposed processes accommodate all needed activities and processes within the digital forensic investigation for a specific case and specific type of the digital forensic investigation?	YES	YES	YES
Did the proposed processes assist the investigators to improve admissibility of digital evidence?	YES	YES	YES
Did the proposed processes assist with effective and efficient collaboration within the digital forensic investigation for a specific case?	YES	NOT CONCLUSIVE	NOT CONCLUSIVE
Did the proposed processes improve on expected efficiency and effectiveness of the digital forensic investigation?	NOT CONCLUSIVE	NOT CONCLUSIVE	NOT CONCLUSIVE

Once again, note that this evaluation is qualitative and performed based on investigators' expert opinions. It can also be noted from the table above that the test cases showed strongly that the proposed processed accommodated all needed activities within the investigations. The proposed processes were applied to three different real-world cases, two being of the mobile digital forensics type and one being of the post-mortem digital forensics type. Therefore, it can be reasonably assumed that the proposed processes are adaptable to different types of digital forensic investigations and that the proposed processes are defined as generic as possible to be applicable to different circumstances of the investigation (for example different scenarios, hardware platforms, operating systems etc.).

Further, from the table above, one can see that the testing cases strongly showed that the proposed processes assist in improving admissibility of the digital evidence. This is achieved through providing clear guidelines on how specific digital forensic principles should be implemented and achieved.

Last, but not least, it can be concluded from the table above that the investigators, while implementing the processes to the real-world cases, could not establish with certainty whether the proposed processes significantly improve efficiency of collaboration (for example, through defined information flows) and whether the proposed processes significantly improve on

expected efficiency and effectiveness of the investigation (for example, through reducing cost or time of the investigation, or through achieving higher success rates of the investigations). Further evaluation will be needed in this regard. The authors plan to conduct further evaluation on larges set of test cases in order to be able to more conclusively confirm potential benefits of the proposed processes.

The following section discusses the results of the paper.

5. DISCUSSION

In this paper the authors proposed several processes to be performed concurrently with the existing processes of the digital forensic investigation process model, in order to achieve better efficiency for and during an investigation as well as to ensure the admissibility of digital evidence. The introduction of the proposed concurrent processes would ensure that digital forensic principles are correctly applied throughout the course of digital forensic investigation and would lead to better efficiency and higher admissibility. Also, the introduction of the proposed concurrent processes would enable planning of their implementation in order to make the investigation more efficient.

The proposed processes processes translate the well-established principles in digital forensics and harmonize existing work in this field.

This is a novel contribution to the digital forensic investigation process and the authors believe that their proposed model can be more functional and effective than existing models. These concurrent processes are an important addition to existing digital forensic investigation process and the authors believe the application of these would enable significantly higher admissibility and efficiency of digital evidence for digital forensic investigations.

The processes proposed within the concurrent processes class are well defined in terms of scope and functions. They are also comprehensive, in that they include all of the digital forensic principles identified in the existing digital forensic investigation process models. Table 1 clearly shows the comprehensiveness of the proposed concurrent processes class, as it translates all of the identified principles into concurrent processes.

The use of the proposed concurrent processes could foster many benefits for digital forensic practitioners and academics. Possible benefits include:

- Higher admissibility of digital evidence in a court of law, because digital forensic principles were applied in a standardized way;
- Human error and omissions during the digital forensic investigation process would be minimized, because it would be less likely for practitioners to omit the application of one of the digital forensic principles;
- The proposed digital forensic investigation process model would enhance the efficiency and effectiveness of digital forensic investigations;
- Training of digital forensic personnel would be easier, especially for the application of the digital forensic investigation principles.

The implementation of the proposed concurrent processes was evaluated on three real world cases. Evaluation has confirmed usability and adaptability of the proposed processes in different types of digital forensic investigations and under different circumstances. Further the evaluation showed that the implementation of the proposed concurrent processes would potentially bring benefits of higher admissibility of digital evidence. The evaluation findings on improving collaboration and improving efficiency and effectiveness of the investigation were not fully conclusive. Further work will be undertaken by the authors to evaluate the implementation of the concurrent processes on larger number of investigations in order to be able to draw more conclusive or event statistical conclusions on the above.

6. CONCLUSION

Let us revisit the problem statement. The problem addressed in this paper was that the existing digital forensic investigation process models do not include processes relating to the application of digital forensic principles that stretch across the duration of a digital forensic investigation, thus creating room for errors, omissions and ultimately for issues with digital evidence integrity. The proposed concurrent processes are aimed at enabling efficient and effective digital forensic investigations, and also work towards increasing the admissibility of digital evidence in any court of law.

The authors believe that the proposed concurrent processes are a significant step towards the harmonization of existing models. The proposed processes represent an important contribution and a novel approach to the principles of digital forensics, and it would ensure that these principles are applied consistently throughout the digital forensic investigation. This in turn ensures digital evidence integrity and thus ensures admissibility. Further the introduction of the proposed concurrent processes promotes efficient and effective investigations.

Future work should include development of application prototypes and further evaluation and testing of the implementation of the proposed concurrent processes. Further evaluation and testing would be performed with and without use of the above mentioned prototype and it would be conducted on a large set of test cases in order to reliably confirm benefits of the proposed introduction of concurrent processes. It is authors' intention to conduct this further testing and evaluation on different types of digital forensic investigations (for example mobile, cloud, post-mortem etc.) in order to fully confirm adaptability of the proposed processes.

REFERENCES

[1] Federal Rules of Evidence, U.S. Government Printing, 2010
[2] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 1993
[3] ACPO, "ACPO good practice guide for computer-based evidence" [ONLINE], Available at: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf , Accessed 18 February 2013
[4] Cybex, The Admissibility of Electronic Evidence in Court, Fighting Against High-Tech Crime (Cybex, Barcelona), 2005
[5] Mason, "International electronic evidence", British Institute of International and Comparative Law, 2008
[6] Palmer G., A road map for digital forensic research; Technical Report DTR-T001-01, DFRWS, November 2001; Report From the First Digital Forensic Research Workshop (DFRWS), 2001
[7] Reith M. et al., An examination of digital forensic models, International Journal of Digital Evidence, 2002
[8] Carrier B. and Spafford E., Getting physical with the digital investigation process, International Journal of Digital Evidence, Vol. 2, 2, [Electronic version], 2003
[9] ISO/IEC 27043:2015, "Information technology – Security techniques – Investigation principles and processes", international standard, 2015
[10] Mandia K. et al., Incident response & computer forensics (Second Ed.), McGraw-Hill/Osborne, Emeryville, 2003
[11] Cuardhuáin S.O., An extended model of cybercrime investigations, International Journal of Digital Evidence, Summer 2004, Volume 3, Issue 1, 2004
[12] Beebe N.L. and Clark J.G., A hierarchical, objectives-based framework for the digital investigations process, Digital Investigation 2(2), 2005
[13] Casey E. and Rose C.W., chapter Forensic analysis in Handbook of digital forensics and investigation, 2010
[14] Cohen F.B. et al., The state of the science of digital evidence examination, 2011
[15] The U.S. Department of Justice, "electronic crime scene investigation – a guide for first responders", 2001
[16] Carrier B. and Spafford E., An event-based digital forensic investigation framework, Digital Investigation 2(2), 2005
[17] ACPO, ACPO good practice guide for computer-based evidence [Internet], United Kingdom, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf, last accessed 18.02.2013, 2008
[18] Cohen F.B., Fundamentals of digital forensic evidence, chapter in handbook of information and communication security [Internet], All.Net, last accessed on 04.01.2011, 2011
[19] http://www.businessdictionary.com/definition/harmonization.html#ixzz3VKmEpZtu [ONLINE]
[20] Removed for purposes of blind review process
[21] Casey E. and Schatz B., Chapter 6 in Digital evidence & computer crime, 3rd Edition, 2011
[22] Removed for purposes of blind review process
[23] Micro Systemation (MSAB) XRY [ONLINE], Available at http://www.msab.com
[24] Removed for purposes of blind review process
[25] Removed for purposes of blind review process
[26] European Police Office, "Internet Organised Crime Threat Assessment (iOCTA) 2014", 2014
[27] Tan J., "Forensic Readiness", Technical. Cambridge USA: @stake, Inc., 2001