Harmonised Digital Forensic Investigation Process Model

Aleksandar Valjarevic
Department of Computer Science,
University of Pretoria
Pretoria, South Africa
alexander@vlatacom.com

Hein S. Venter
Department of Computer Science,
University of Pretoria
Pretoria, South Africa

Abstract— **Digital forensics gained significant importance over the past decade, due to the increase in the number of information security incidents over this time period, but also due to the fact that our society is becoming more dependent on information technology. Performing a digital forensic investigation requires a standardised and formalised process to be followed. There is currently no international standard formalising the digital forensic investigation process, nor does a harmonised digital forensic investigation process exist that is acceptable in this field. This paper proposes a harmonised digital forensic investigation process model. The proposed model is an iterative and multi-tier model. The authors introduce the term "parallel actions", defined as the principles which should be translated into actions within the digital forensic investigation process (i.e. principle that evidence's integrity must be preserved through the process and that chain of evidence must be preserved). The authors believe that the proposed model is comprehensive and that it harmonises existing state-of-the-art digital forensic investigation process models. Furthermore, we believe that the proposed model can lead to the standardisation of the digital forensic investigation process.**

Keywords- information systems security, digital forensics, process, model

I. INTRODUCTION

Digital forensics is gaining importance rapidly. Information security incidents constantly highlight the importance of digital forensics. The fact that societies depend heavily on information technology, contributes to importance of digital forensics.

Digital or electronic evidence comprises information and data of investigative value stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA evidence is latent [2]. Dealing with digital evidence, therefore, requires a standardised and formalised process in order for digital evidence to be accepted in a court of law. Methods and process models for digital forensic investigation process have been developed mostly by practitioners and forensic investigators, based on personal experience and expertise, on ad hoc bases, without the aim to reach harmonisation or standardisation 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. There is, however, currently no international standard formalising the digital forensic investigation process, although an effort to standardise the process has started within International Standardisation Organisation (ISO), by the authors [3].

It is with this in mind that authors defined the following problem statement. The problem is that there is currently no harmonised digital forensic investigation process model that can be used as a standardised set of guidelines for digital forensic investigation.

Providing guidelines for investigation process should expedite investigations because there would be proper guidelines in the order of events during an investigation. Such guidelines would also be a good departure point to encourage the training of inexperienced investigators. The need for a harmonised digital forensic investigation process model is most prominently seen in a court of law. In order to be able to claim in court that a standard process was used during digital forensic investigation, a harmonised digital forensic investigation process model should exist and be adhered to. As an example, Daubert rule [4], most prominently used in the USA for expert witness testimony, including digital forensics experts clearly states that theories and techniques used to draw conclusions on case must give positive answer to the following questions:whether the theories and techniques employed by the scientific expert have been tested;whether they have been subjected to peer review and publication;whether the techniques employed by the expert have a known error rate;whether they are subject to standards governing their application; and whether the theories and techniques employed by the expert enjoy widespread acceptance.

This clearly indicates need for harmonised and ultimately standardised digital forensic process.

The paper is structured as follows: The first section has introduced the paper and provided the problem statement. Section II gives background on digital forensics, legal requirements regarding the digital forensic investigation process and past work on the digital forensic investigation process. After that, Section III explains a proposed Harmonised Digital forensic investigation process Model, while Section IV concentrates on discussing the proposed

process. Section V concludes this paper and indicates possible future work.

II. BACKGROUND

A. On Digital Forensics

In this section the authors wish to give definition of digital forensics.

Digital forensics is defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations [2].

B. Legal Requirements

In this section the authors give an overview of the legal requirements 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 harmonised, and ultimately, a standardised digital forensic investigation process. It should be noted that 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 should be adopted by the legal system of a specific jurisdiction.

For example, in the United Stated of America 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 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." For application of this rule, the Daubert case [4] is the most important. Other countries have similar requirements regarding the admissibility of digital evidence. 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] [7].. The European Committee on Crime Problems (CDPC), known as the Committee of Experts on Crime in Cyber-Space (PC-CY), finished a draft convention on cyber-crime. This convention makes numerous references to the collection and exchange of electronic evidence [5]. The final AEEC (Admissibility of Electronic Evidence in Court) Conference provided an overview of the results of the Admissibility of Electronic Evidence in Court project that had been partly funded by the European Union. A number of those present at the conference expressed the view that it would be good to have a European-wide law on electronic evidence for criminal proceedings [8] [9].

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

C. Related Work on Digital Forensic Investigation Process Model

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 [2], the need for a standard framework for digital forensics has been widely. The digital forensic investigation process model proposed at this workshop includes the following seven phases: Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision. The process model was defined as iterative.

Reith, Carr and Gunsch [10] proposed a digital forensic investigation process model known as the abstract model, which includes the following phases: 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 phases: 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 phase 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 phases organised into the following five groups: readiness phases, deployment phases, physical crime scene investigation phases, digital crime scene investigation phases and review phase.

Carrier and Spafford also proposed another (similar) event-based process model [13]. 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 phases and how to find the causes and effects of events during a digital forensic investigation.

Mandia and Prosise [14] proposed a digital forensic investigation process known as the incident model, which

contains the following phases: 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 phase), reporting and follow-up.

Beebe and Clark [15] 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 phases proposed in [15] include the following: preparation, incident response, data collection, data analysis, findings presentation and closure. In their opinion, second-tier sub-phases should be defined in such a way that these are inclusive of all possible types of crime and types of digital evidence.

Cuardhuain [16] proposed an extended and comprehensive model of cybercrime investigations, which is very comprehensive. The proposed model also includes information flow description between different phases.

Cohen [17] proposed a process model that includes the following phases: identification, collection, preservation, transportation, storage, analysis, interpretation, attribution, reconstruction, presentation and destruction.

Casey and Rose [18] define phases 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, Lowrie and Preston in [19] discuss the state of the science of digital evidence examination and consensus in digital evidence examination. These authors recognise that numerous calls have been made for scientific approaches and formal methods in the field of digital forensics [19] [20] [21] [22] [23] [24] [25].

As previously said, 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] [7]. These guidelines do not explicitly set out digital forensic investigation process model, but through recommendations given process model can be constructed, containing following phases: preparations for investigation, crime scene group of phases, secure and control the crime scene, photograph and document the scene, initial collecting of volatile data, attaching exhibit labels, documenting each action performed, transport, storage, evidence recovery group of phases, the collection phase, the examination phase, the analyses phase, the reporting phase, 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 phases included, the scope of models, and the scope of similarly named phases 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). The authors also note that they are of the opinion that body of knowledge and peer reviewed papers on digital forensic investigation process are scarse and that experts and practitioners in the field should concentrate more on this subject.

Our proposal for a harmonised digital forensic investigation process model is presented in the next section.

III. PROPOSING HARMONISED DIGITAL FORENSIC INVESTIGTION PROCESS MODEL

The paper defines a digital forensic investigation process model aimed at harmonising existing models. The model that is proposed is generic enough to be used for different digital forensic investigations and different types of digital evidence. Also, the model is comprehensive, meaning that it is inclusive of the benefits of previous models. The model inherits most of the phases proposed by other authors and in that sence it is comprehensive, but it proposes different organisation of the phases and introduces a novel approach to implementation some of digital forensic principles through actionable items calls *parallel actions*. . We define parallel actions as the principles which should be translated into actions within the digital forensic investigation process (i.e. principle that evidence's integrity must be preserved through the process and that chain of evidence must be preserved). These principles are found in one or more existing models. While in most of the models analysed, these are defined as principles, there are cases where these principles have already been translated to actions in the form of a phase in the model (i.e. in [12] the principle that there should be interaction with physical investigation of the actual crime scene is translated in *physical crime scene investigation group of phases*).

Phases have been selected based on previous work in this field and an attempt was made to harmonise the phases described by other authors. The following principle was used to distinguish between different phases: A set of activities can be defined as a phase if all activities have a common aim and if activities last for a limited period of time, compared to the time needed for a whole digital forensic investigation process.

We also propose the introduction of six actions that run parallel with the phases (*parallel actions*). These actions are aimed to achieve highest efficiency of the investigation and the admissibility of digital evidence. They are based on principles that need to be followed during a digital forensic investigation and actions that have a wider scope than a single phase. We believe that by having this principles translated to actionable items it will be easier for practitioners to strictly adhere to these.

The proposed model comprises the following twelve phases: incident detection, first response, planning, preparation, incident scene documentation, potential evidence identification, potential evidence collection, potential evidence transportation, potential evidence storage, potential evidence analysis, presentation and conclusion. We propose a multi-tiered model, where each phase would contain a set of sub-phases. The authors believe that sub-phases can only be fully defined for a specific type of incident and investigation. Legislative rules would also have a high impact on the definition of sub-phases. The proposed phases of our model are next described in more detail.

A. Incident Detection Phase

Incident detection procedures must be in place prior to the beginning of this phase. 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/administering information systems detect an incident. Examples of external incident detection systems are intrusion detection systems, intrusion prevention systems, log-analysing systems, change-tracking systems, etc. The incident detection phase includes detection of the incident, but also includes 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 'unauthorised access to the *root* account of the operating system', than if it was described as 'using the computer to distribute child pornography'. Based on the above, this phase would consist of three sub-phases: incident detection, incident classification and incident description. It is important here that incident classification and description must be performed based on information gathered prior to incident detection and should not include any action that might alter data at the target system. If there is digital forensic readiness process for the target information system it will represent an input to this phase. Incident detection activities were defined since DFWRS [2] (as part of Identification phase), but Mandia et al. [14] were the first to define these in separate phase. 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 phase as a first phase in the model and not a preparation or planning phase, 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.) There for our process model starts with incident detection and later preparation and planning phases are concerned with digital forensic investigation process rather than with digital forensic readiness process.

B. First Response Phase

The first response phase should include the first response to the detected incident. If there is digital forensic readiness process for the target information system it will represent an input to this phase. Depending on the type and severity of the incident, this might include disconnecting equipment from a networked environment, detecting corrupted data, etc. It is desirable that the first response does not have a negative influence on the possibility to perform a digital forensic investigation, i.e. not to include powering-off the equipment, opening or changing files etc. Defining first response actions is out of the scope of this document, as these can vary greatly depending on type of target information systems, data contained in target information system, circumstances of the incident, classification and description of the incident etc. Mandia et al. [14] and Beebe et al. [15] have included incident response phases in their models as initial response and incident response, respectively. The authors have chosen to include this phase 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)

C. Planning Phase

During this phase one has to perform all the planning needed 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 phases. If digital forensic readiness measures were implemented, one should plan how to use the results of these measures so as to maximise the success of the digital forensic investigation process. During the planning phase an interface should be defined between the digital forensic readiness process and the digital forensic investigation process. The aims of the digital forensic readiness process are to maximise the potential use of digital evidence, minimise the costs of investigation, minimise interference with and prevent the interruption of business processes, and to preserve or improve the current level of information systems security. Note that digital forensic readiness is not included in the proposed process model and that it is a completely separate process. In our proposed process model we just emphasise the need to define an interface between the two processes. The planning phase is of extreme importance because it determines the efficiency and success of all the other phases. Many authors have chosen to include this phase, although often as the first phase. Reasoning for our choice

to place it here, as third phase, was given in "*A. Incident detection phase*" section.

D. Preparation Phase

Preparation phase activities are intended to prepare an organisation for performing the activities of other digital forensic investigation process phases. 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 phase, preparations also have to be made to implement procedures defined in the previous phase. Many authors have chosen to include this phase, although often as second phase in sequence. Reasoning for our choice to place it here, as forth phase, was given in in "*A. Incident detection phase*" section.

E. Incident Scene Documentation

This phase is performed at the scene of the incident and involves the proper documentation of the complete incident scene, including written documentation of actions, scatches, photographs, videos, labeling the potential evidence. All actions performed in relation to the digital forensic investigation process should be recorded, together with details on the architecture and components of the information system where the incident occurred. DOJ [11], Carrier et al. [12] and ACPO [6] have included this phase in their digital forensic investigation process models. The authors have chosen to include this phase, because they find it is of highest importance for preservation of chain of evidence and preparation for ultimate presentation of the investigation findings. We believe that it should exist as a separate phase, as it has different aim from other activities performed at incident scene.

F. Potential Evidence Identification Phase

This is the second phase performed at the scene of the incident. Although it overlaps in time with the previous phase, we as authors consider it as a separate phase because it includes different types of action, with different aim. Cohen [17] says: "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 evidence at the incident scene is of crucial importance for the rest of the process, because if evidence is not identified at this point, it might not even exist at a later point. This is especially important when an incident happens in a networked environment, in an environment where live forensics should be performed, in cloud environment or in an environment with exceptionally large amounts of data. Reith et al. [10], DOJ [11], Carrier et al. [12], Cuardhuain [16], Cohen [17], Casey and Rose [18] and ACPO [6] have included this phase in their respective models, some with different name and with different scope. The authors believe that *Potential evidence identification phase* should be a separate phase, with sole aim to identify potential evidence.

G. Potential evidence collection phase

Once potential digital evidence has been identified, it has to be collected in order to permit its analysis in a later phase. 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 court. Adhering to strict legal regulations during the evidence collection phase is of crucial importance, as digital evidence might become unusable when proper procedures are not followed. It is common practice to take forensically sound images of all the bits contained within each media that comprises potential digital evidence. Professionals and scientists in the digital forensics field have a task to develop proper procedures for the collection of potential evidence that is applicable to networked environments, the live forensic process, cloud environments and environments with large amounts of data.It is notable that many authors [2] [10] [17] have proposed two separate phases instead of ours c*ollection phase*. Namely they propose separate collection and preservation phases. However the authors believe that this should be a single fase as aim is single, to collect potential evidence, while preserving the evidence is more of a principle to be followed. Other authors, such as [6] [14] break down this phase to few other phases. In [6] these are *initial collecting of volatile data* and *the collection phase*. However we believe that again there is a single aim of these two phases, to collect potential evidence, and it should not be broken down to several phases based on whether you collect different type of evidence or use different type of tool.

H. Potential Evidence Transportation Phase

During this phase, potential digital evidence is to be transported to a location where it is to be stored and later analysed. 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 evidence, such as encrypting and digitally signing data. In [6], [11], [16], [11] and [18] this is included as a separate phase. This should exist as a separate phase on a basis that activities performed have a single aim, not shared with other phases, to securely transport the potential evidence to the location where analyses would be performed, while obliging to principle of preserving the evidence.

I. *Potential Evidence Storage Phase*

The storage of digital evidence might be needed if analyses 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 phase. Care must also be taken not to damage the media carrying digital evidence due to shock, temperature, humidity, pollution, loss of power, malfunction, etc.

In [6], [16], [17] this is included as a separate phase. This should exist as a separate phase on a basis that activities performed have a single aim, not shared with other phases, to securely and safely store the potential evidence.

J. *Potential Evidence Analysis Phase*

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 analysed in present-day digital forensics, the analysis of evidence becomes a challenge. As volumes of data to be analysed can be vast, automated techniques are often employed to complement manual analysis techniques. Most of the authors have split scope of our *analysis phase* to several separate phases. For example DFWRS [2] and DOJ [11] split it in *examination* and *analyses* phases. ACPO [6] model has three separate phases, namely: The analyses phase, The examination phase and The reporting phase, to cover the scope of our *analyses* phase. Cohen [17] has the most granular approach and has four separate phases: analyses, interpretation, attribution and reconstruction. The authors have decided to propose a single *Analyses* phase, whose aim would be to produce hypothesis about incident occurrence and to find appropriate digital evidence to support the hypothesis.

K. *Presentation Phase*

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.) Such evidence should 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 presentation can be made in the form of a written report, multimedia presentation, expert witness testimony, etc. The presentation phase 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.

L. *Conclusion Phase*

This phase concludes the digital forensic investigation and a decision is to be made on the validity of the hypothesis set in the presentation phase. As stated earlier, the proposed digital forensic investigation process model is iterative. This implies that – after completing this phase – one can go back to any of the earlier phases that follow the incident detection phase. The conclusion phase should include the following actions (sub-phases): acceptance or rejection of hypothesis, returning evidence, if needed, destruction of evidence, if needed, distribution of relevant information to all stakeholders. 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, but often with more limited scope then as it is defined in the proposed model

M. *Parallel Actions*

The proposed digital forensic investigation process model also includes the following actions that should be taken in parallel with the phases proposed above: obtaining authorisation, documentation, defining the information flow, preserving the chain of evidence, preserving evidence and interaction with the physical investigation. These actions are translation of well established and adopted principles of digital forensics into actionable items.

The parallel actions suggested above are justified, as we strongly believe that the principles of the digital forensic investigation process, as well as the preservation of the evidence and the chain of evidence must be translated into actionable items. These actions should run parallel with all other phases in order to ensure full admissibility of the digital evidence in court. Moreover, actions that have been defined in previous works in a phase approach (such as obtaining authorisation, documentation and interaction with physical evidence) must actually run across several or all phases. The aim of these parallel actions is to achieve higher efficiency of the investigation. The authors also believe that information flow should be defined as a separate parallel action. Some of the authors have defined one or more of these actions as a digital forensic process model phases, i.e. in [16] *obtaining auhorisation* is defined as a model phase. However we firmly believe that this actions span across several phases, often throughout complete timeline of the process model and as such can not be defined as a phase in the model. The proposed actions are explained next.

1) Interaction with the physical investigation [6] [12]

The authors note that the digital forensic process can be dependent on and interconnected with the physical investigation of the actual crime scene, if such an investigation is conducted in relation to the same incident. The authors define physical crime scene investigation as investigation of actual crime scene performed using traditional forensic and investigation methods. Therefore, there should be a principle to define the relationship between the digital forensic investigation process and the physical investigation. The interaction with the physical crime scene investigation is important for preserving the chain of evidence, preserving the integrity of the digital evidence, protecting the digital evidence from damage and ensuring an efficient investigation.

2) Preserving the chain of evidence [4] [6] [10] [11] [12] [14] [15] [16] [17] [18]

All legal requirements must be complied with and all actions be properly documented in order to preserve the chain of evidence as well as the integrity of the digital evidence. This principle must be followed during the entire course of the digital forensic investigation.

3) Preserving evidence [4] [6] [10] [11] [12] [14] [15] [16] [17] [18]

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 importantly, it must be guaranteed that no opportunity arises during the entire investigation in which the original evidence may be tampered with.

4) Information flow [6] [16]

It is important to identify and describe these information flows so that they can be protected and supported technologically, for instance through the use of trusted public key infrastructures and time stamping to identify investigators and authenticate evidence. [16] A defined information flow should exist between each of the phases of the process and among different stakeholders, including investigators, managers and external organisations. Information flows should be also defined with sources of information of importance, such as relevant policies, technology information etc.

5) Documentation [6] [6] [10] [11] [12] [14] [15] [16] [17] [18]

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

6) Obtaining auhorisation [6] [12] [16]

Proper authorisation should be obtained for each action performed within all of the phases. Authorisation might be required from government authorities, system owners, system custodians, principals, etc.

N. Digital forensic investigation process model schema

Figure 1 below represents the digital forensic investigation process model schema. As can be noted, phases are sequential – with the exception of the incident scene documentation and evidence identification phases, which may overlap in time. Also, note that not all parallel actions run together with all of the phases. For instance, p*reserving chain of evidence*, p*reserving evidence* and i*nteraction with physical investigation* actions start only with f*irst response* phase. The proposed process model is defined as iterative, which implies that after the last phase one can return to previous phase. Note, however, that iteration is optional and that one can only return to earlier phase after first response phase.

O. New definition of digital forensics

The authors would like to modify the widely used definition [2] of digital forensics to the following, based on proposed digital forensic investigation process model: “Digital forensics is defined as the use of scientifically derived and proven methods towards the identification, collection, transport, storage, analysis, presentation and distribution and/or return and/or destruction of digital evidence derived from digital sources, while obtaining proper auhorisation for all actions, properly documenting all actions, interacting with physical investigation, preserving the evidence and the chain of evidence, for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations”

I. Comparison of Existing Models to the Proposed Harmonised Digital forensic investigation process Model

In this section, existing models are compared with the proposed harmonised digital forensic investigation process model (see Table 1). The proposed process model will be mapped to existing models.

The proposed model is iterative and multi-tiered. Sub-phases of the proposed model are not shown on the comparison table for the sake of simplicity of view. Each mapped phase starts with a number, marking a sequence of phases within the model with which comparison is being made. Note that the authors envisage that, ideally, all planning of actions (planning, defining of the approach strategy, defining of the response strategy, etc.) should be done prior to the incident – thus during the planning phase.

Based on the comparison made in Table 1, we as authors claim the comprehensiveness of our proposed model. We

also introduced the ‘parallel actions’ principle, as it would ensure higher efficiency and digital evidence admissibility. Note also that the order of the phases defers from some of the previous models and that the authors believe that the proposed order makes provision for a more efficient process and following of the claims made by the authors, such as that digital forensic readiness process should be kept separate from digital forensic investigation process and that incident detection and first response should be included in digital forensic investigation process. The authors strongly believe that in order to have a fully harmonised model, a comprehensive analysis has to be made of national and international police (and other institutions performing investigations) processes and procedures in the field of digital forensics. A future harmonised digital forensic investigation process model will have to take into account practices of investigating institutions on a national and international level in order for the model to be practically applicable. The authors will include this as future work.

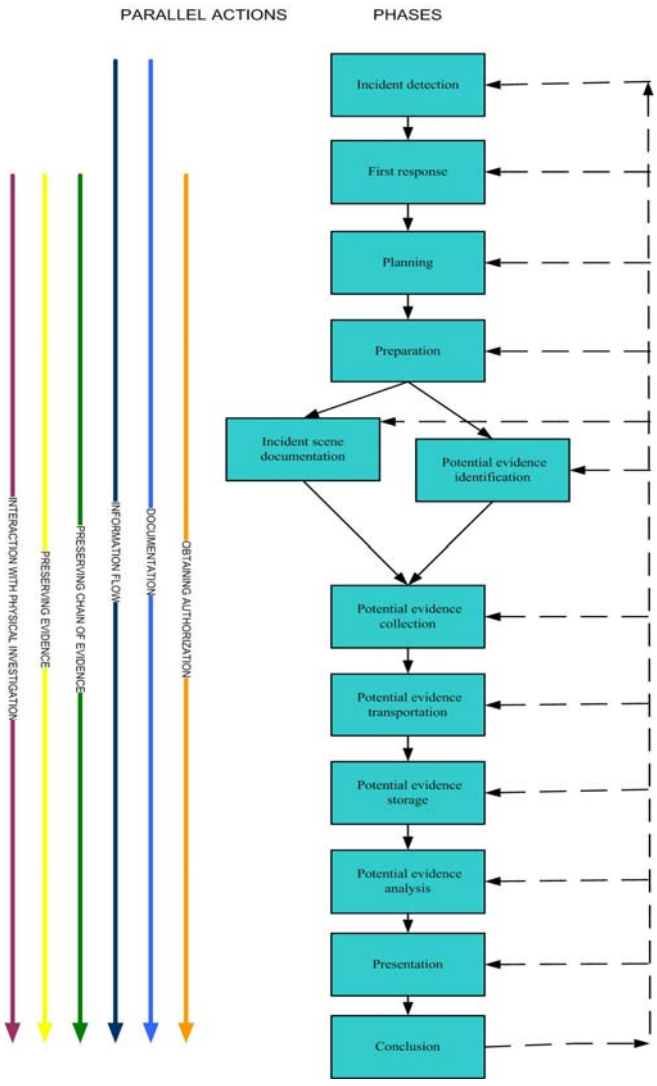

Figure 1: Digital forensic investigation process model schema

IV. Discussion

Our proposed digital forensic investigation process model is comprehensive and inclusive of all the benefits conveyed by previous models. The phases in the proposed model are well defined in terms of scope, functions and order. In this paper we also proposed several actions to be performed constantly and in parallel with the phases of the model, in order to achieve efficiency of investigation and ensure the admissibility of digital evidence. These actions translate the well established principles in digital forensics. This is a novel approach to digital forensic investigation process and the authors believe that it can be more functional and effective than existing models.

Use of the proposed harmonised digital forensic investigation process model could bring about multiple benefits. A first benefit would be the higher admissibility of digital evidence in a court of law, due to the fact that a standardised process was used. Also, human error and omissions during the digital forensic investigation process would be minimised once such a harmonised 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. Last, but not least, the authors strongly believe that the proposed digital forensic investigation process model would enhance the efficiency and effectiveness of digital forensic investigations.

V. Conclusion

Let us revisit the problem statement. “The problem is that there is currently no harmonised digital forensic investigation process model that can be used as a standardised set of guidelines for digital forensic investigation.” (See Section I.) Our proposed model is an endeavor to harmonise existing models, while at the same time complying with legal recommendations and requirements. It aims at enabling efficient and effective digital investigation, and also works towards increasing the admissibility of digital evidence in any court of law. The proposed model should be used by scientists and practitioners in the field in their attempt to adopt harmonised and standardised digital forensic investigation process model. Claims made in this paper are to be verified through an appropriate prototype as future work. Future work should also include the development of more procedures to be included as guidelines for the model implementation in respect of different types of digital forensic investigation and different types of digital evidence. The development of more sub-phases on the second tier of the proposed model could also be considered in future research.

TABLE 1: COMPARISON OF EXISTING MODELS TO THE PROPOSED HARMONISED MODEL

	Reference phases	DFWRS [2]	Reith et al. [10]	DOJ [11]	Carrier et al. [12]	Mandia et al. [14]	Beebe et al. [15]	Cuardhuain [16]	Cohen [17]	Casey and Rose [18]	ACPO [6]
Phases											
1	Incident detection	1. Identification	1. Identification		2. Detection and notification	2. Detection of the incident3. 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 phases	4. Response strategy formulation	1. Preparation				1. Preparations for investigation
4	Preparation		2. Preparation	1. Preparation	1. Readiness group of phases	1. Pre-incident preparation		3. Planning			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 exhibit labels
6	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 phase
7	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 phase
8	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	Evidence analysis	4. Examination 5. Analysis	7. Analysis	6. Examination 7. Analysis	4.4 Search for digital evidence 4.5 Digital crime scene reconstruction	6. Investigation	4. Data analyses	9. Examination of evidence 10. Hypothesis	6. Analyses 7. Interpretation 8. Attribution 9. Reconstruction	2. Form a hypothesis to explain observations 3. Evaluate the hypothesis 4. Draw conclusions and communicate findings	5.2 The analyses 5.3 The examination 5.4 The reporting
11	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	
12	Conclusion	7. Decision	9. Returning evidence			9. Recovery 11. Follow-up	6. Closure	13. Dissemination of information	11. Destruction		6. Disclosure
Actionable principles											
1	Interaction with physical investigation				3. Physical crime scene investigation group of phases. Complete crime scene investigation is included in the proposed model.						As principle and set of actions, including preservance of physical evidence and interviews
2	Preserving chain of evidence	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
3	Preserving evidence	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
4	Information flow							Present			Present
5	Documentation	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
6	Obtaining authorisation				2. Confirmation and authorisation			Present			Present

REFERENCES

[1] Tan, J. (2001), "Forensic readiness", Technical. Cambridge USA: @stake, Inc.

[2] Gary Palmer (2001), "A Road Map for Digital Forensic Research". Technical Report DTR-T001-01, DFRWS, Report From the First Digital Forensic Research Workshop (DFRWS).

[3] ISO/IEC 27043, "Investigation principles and Processes", unpublished draft international standard (2012).

[4] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

[5] Pollitt, M.M. (2001), "Report on digital evidence", 13th Interpol Forensic Science Symposium, Lyon, France.

[6] "ACPO Good Practice Guide for Computer-Based Evidence"(2008), http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

[7] http://en.wikipedia.org/wiki/Digital_evidence

[8] The Admissibility of Electronic Evidence in Court (2005), Fighting Against High-Tech Crime (Cybex, Barcelona).

[9] Stephen Mason (2008), "International Electronic Evidence", British Institute of International and Comparative Law.

[10] M. Reith, C. Carr and G. Gunsch (2002), "An examination of digital forensic models", International Journal of Digital Evidence.

[11] The U.S. Department of Justice (2001), "Electronic Crime Scene Investigation- A Guide for First Responders".

[12] Carrier B. and Spafford E. (2003), "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, Vol. 2, 2, [Electronic version].

[13] Carrier B. and Spafford E. (2005), "An Event-Based Digital Forensic Investigation Framework", Digital Investigation 2(2).

[14] Mandia, Kevin, Prosise, Chris and Pepe (2003), "Incident Response & Computer Forensics" (Second Ed.), McGraw-Hill/Osborne, Emeryville.

[15] Nicole Lang Beebe and Jan Guynes Clark (2005), "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process", Digital Investigation 2(2).

[16] Séamus, Ó. and Cuardhuáin, (2004), "An Extended Model of Cybercrime Investigations", International Journal of Digital Evidence, summer 2004, Volume 3, Issue 1.

[17] Frederick B. Cohen (2011), "Fundamentals of Digital Forensic Evidence, Chapter in Handbook of Information and Communication Security", accessed at all.net on 04.01.2011.

[18] Eoghan Casey and Curtis W. Rose (2010), chapter "Forensic Analysis " in "Handbook of Digital Forensics and Investigation"

[19] Frederick B. Cohen, Julie Lowrie and Charles Preston (2011), "The State of the Science of Digital Evidence Examination", all.net.

[20] R. Leigland and A. Krings (2004), "A Formalisation of Digital Forensics", International Journal of Digital Evidence, fall 2004, Volume 3, Issue 2.

[21] Ryan Hankins, T. Uehara and J. Liu (2009), "A Comparative Study of Forensic Science and Computer Forensics", Third IEEE International Conference on Secure Software Integration and Reliability Improvement.

[22] Committee on Identifying the Needs of the Forensic Sciences Community (2009), "Strengthening Forensic Science in the United States: A Path Forward", ISBN: 978-0-309-13130-8, 254 pages. Committee on Applied and Theoretical Statistics, National Research Council.

[23] Scientific Working Group on Digital Evidence (SWGDE) (2009), Position on the National Research Council Report to Congress – Strengthening Forensic Science in the United States: A Path Forward

[24] S. Garfinkel, P. Farrella, V. Roussev and G. Dinolt, (2009), "Bringing science to digital forensics with standardised forensic corpora", Digital Investigation 6 S2-S11.