A Harmonized Process Model for Digital Forensic Investigation Readiness

Aleksandar Valjarevic, Hein Venter

Chapter 5

A HARMONIZED PROCESS MODEL FOR DIGITAL FORENSIC INVESTIGATION READINESS

Aleksandar Valjarevic and Hein Venter

Abstract Digital forensic readiness enables an organization to prepare itself to perform digital forensic investigations in an efficient and effective manner. The benefits include enhancing the admissibility of digital evidence, better utilization of resources and greater incident awareness. However, a harmonized process model for digital forensic readiness does not currently exist and, thus, there is a lack of effective and standardized implementations of digital forensic readiness within organizations. This paper presents a harmonized process model for digital forensic investigation readiness. The proposed model is holistic in nature and properly considers readiness and investigative activities along with the interface between the two types of activities.

Keywords: Digital forensic investigation readiness, process model

1. Introduction

We are living in an information society where we depend heavily on information systems and information technology. Therefore, we also depend on information systems security, specifically the confidentiality, integrity and availability of data, services and systems. These facts, combined with the increasing rate of information security incidents, make the field of digital forensics even more important.

Methods and process models for the digital forensic investigation process (DFIP) have been developed mostly by practitioners and forensic investigators based on their expertise and experience. The initial goal was to increase the effectiveness and efficiency of investigations, not necessarily to achieve harmonization or standardization. The same is true for the digital forensic investigation readiness process (DFIRP). There is

no international standard that formalizes DFIP or DFIRP. However, at the time of writing this paper, an effort to standardize DFIP and DFIRP has been initiated by us within the International Standardization Organization (ISO). At this time, the standard is in its third working draft and is titled "ISO/IEC 27043 Information Technology – Security Techniques – Investigation Principles and Processes" [5]. Note that ISO/IEC 27043 is considering DFIRP as an integral part of DFIP and, ultimately, DFIRP should be contained within DFIP, i.e., within a single holistic DFIP model.

The focus of this paper is on a DFIRP implementation, not on the entire holistic implementation of DFIP as described in ISO/IEC 27043. The fundamental problem is that no harmonized DFIRP currently exists. This means that organizations do not have clear guidance on how to implement digital forensic investigation readiness.

Guidelines provided by a DFIRP model could enable organizations to better utilize their resources and achieve better results when implementing digital forensic readiness and when performing digital forensic investigations. The DFIRP model would help raise awareness and enhance training efforts related to digital forensic readiness and digital forensic investigations. Moreover, the model could enhance the quality of incidence response and investigations, and the admissibility of digital evidence.

2. Background

This section provides an overview of previous work related to digital forensic readiness, and models and processes used to achieve digital forensic readiness. This discussion is important because the existing digital forensic readiness models are inputs to the proposed harmonized model. Indeed, the proposed model attempts to harmonize existing models.

Digital forensics is the use of scientifically-derived and proven methods for 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 authorization for all actions, properly documenting all actions, interacting with the physical investigation, preserving evidence and the chain of evidence, for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping anticipate unauthorized actions that may disrupt operations [11]. Digital forensic readiness is the ability of an organization to maximize its potential to use digital evidence while minimizing the costs of an investigation [10].

Tan [10] has identified several factors that affect digital forensic readiness: how logging is done, what is logged, intrusion detection, digital forensic acquisition and digital evidence handling. Yasinsac and Manzano [7] have proposed six policy areas to facilitate digital forensic readiness: retaining information, planning the response, training, accelerating the investigation, preventing anonymous activities and protecting evidence. Wolfe-Wilson and Wolfe [12] emphasize the need for an organization to have procedures in place to preserve digital evidence in the event that a digital forensic investigation must be conducted.

Rowlingson [9] defines a number of goals for digital forensic readiness: gather admissible evidence legally and without interfering with business processes, gather evidence targeting the potential crimes and disputes that may adversely impact an organization, allow an investigation to proceed at a cost in proportion to the incident and ensure that the evidence makes a positive impact on the outcome of a legal action. Rowlingson's approach is closely related to our DFIRP model. His key activities when implementing digital forensic readiness are to: define the business scenarios that require digital evidence, identify the available sources and different types of potential evidence, determine the evidence collection requirements, establish a capability for securely gathering legally admissible evidence, establish a policy for secure storage and handling of potential evidence, implement monitoring to detect and deter major incidents, specify circumstances when escalation to a full investigation should be launched, train staff in incident awareness so that they understand their roles in the digital evidence process and the legal sensitivity of evidence, document an evidence-based case that describes the incident and its impact, and ensure legal review to facilitate actions in response to the incident.

Since the first Digital Forensic Research Workshop (DFRWS) [8], the need for a standard framework for digital forensics has been acknowledged by the digital forensics community. A framework for digital forensics must be flexible enough to support future technologies and different types of incidents. Therefore, it needs to be both simple and abstract. However, if it is too simple and too abstract, then it is difficult to create tool requirements and test procedures for the various phases [3].

Several researchers have proposed digital forensic models that include forensic readiness as a phase. However, to the best of our knowledge, no DFIRP model has as yet been proposed.

Carrier and Spafford [2] have proposed a digital investigation process model comprising seventeen phases divided into five groups, one of the groups focusing on forensic readiness; this group incorporates two phases, the operation readiness phase and the infrastructure readiness

phase. Mandia, *et al.* [6] have also proposed a digital investigation process model that includes a readiness phase, known as the pre-incident preparation phase. Beebe and Clark [1] have proposed a hierarchical, objectives-based framework for digital investigations, which includes a preparation phase; this phase encompasses activities designed to achieve digital forensic readiness.

3. Harmonized DFIRP Model

This section describes the proposed harmonized DFIRP model that is intended to provide guidance on implementing digital forensic readiness.

3.1 Aims and Policy

The harmonized DFIRP model has certain aims that are collectively drawn from previous work in the area [3, 7–10, 12]. In particular, the harmonized DFIRP model should:

- Maximize the potential use of digital evidence.
- Minimize the costs incurred in digital investigations.
- Minimize the interference to and prevent the interruption of business processes.
- Preserve or improve the current level of information security.

The fourth aim listed above was not identified in previous work. We believe that this aim is essential when implementing forensic readiness, and even more so when creating a DRIFP model. The first two aims concentrate on the efficiency of investigations and the third aim focuses on non-interference with business processes. Omitting the fourth aim could leave room for flaws in the overall information security status of an organization.

An example of such a flaw is when an organization, based on the first three aims, decides to collect logs from its information systems and maintain them at a central location. However, the organization does not implement security mechanisms to protect the data from compromise or dissemination. A holistic approach that applies information systems security mechanisms to forensic readiness is vital. In fact, forensic readiness should have built-in security features and security should not merely be an add-on.

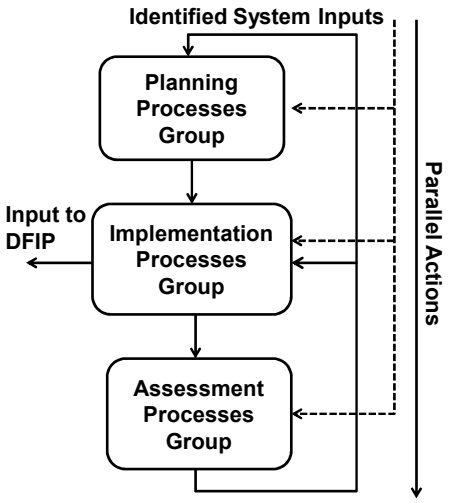

Figure 1. Harmonized DFIRP model: Process groups.

3.2 Model Description

This section describes the proposed DFIRP model in detail. Unlike related work [1] that uses the term "phases," we use the term "processes" in line with ISO terminology [4].

The harmonized model comprises three distinctive process groups: (i) planning processes group; (ii) implementation processes group; and (iii) assessment processes group. Figure 1 shows the three process groups.

The planning processes group includes all the model processes that are concerned with planning activities, including the scenario definition process, source identification process, planning pre-incident collection process, planning pre-incident analysis process, planning incident detection process and architecture definition process. These processes are shown in Figure 2.

The implementation processes group includes only the implementation processes and a link to the harmonized DFIP [11]. The implementation processes group includes the following processes: implementing architecture definition process, implementing pre-incident collection process, implementing pre-incident analysis process and implementing incident detection process. These processes, which are shown in Figure 2, are concerned with the implementation of the results of the planning processes.

The assessment processes group includes two processes, the assessment of implementation process and the implementation of assessment results process.

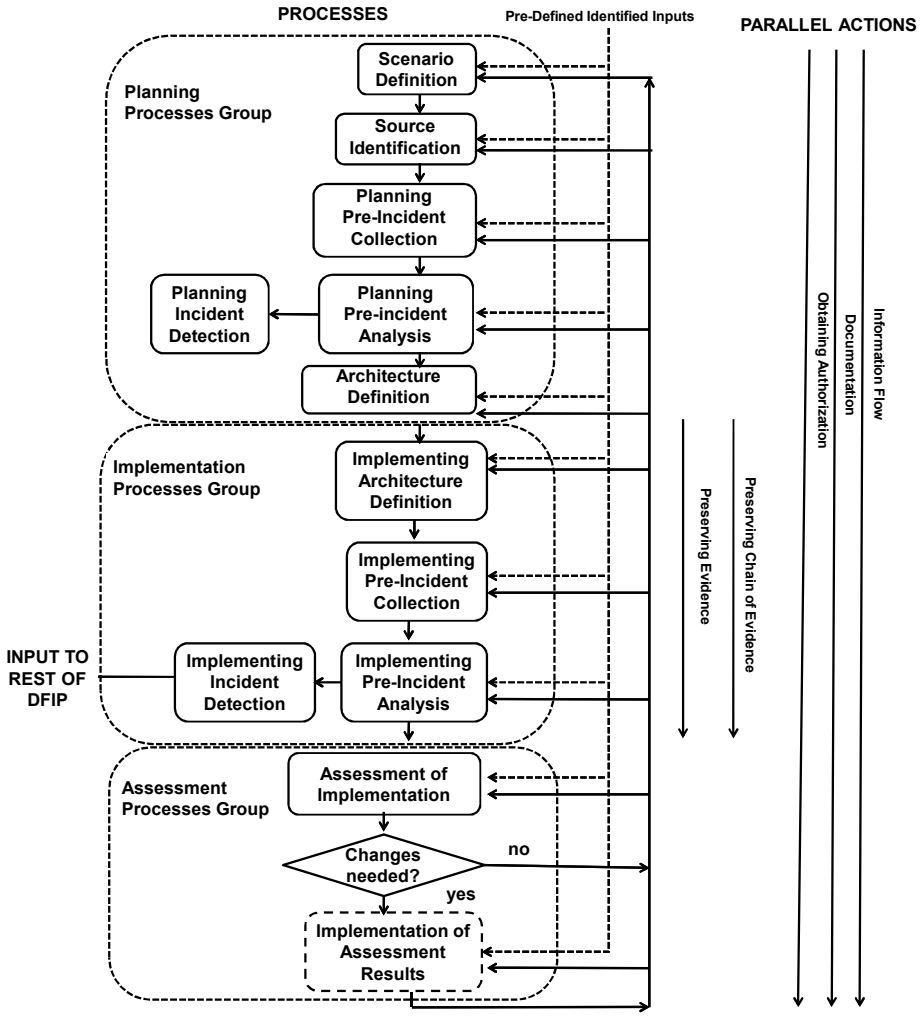

Figure 2. Harmonized DFIRP model.

The harmonized process model also introduces a novel addition to the process model – the concept of parallel actions. We define parallel actions as the principles that should be translated into actions throughout the DFIRP model. As shown in Figure 1, these actions run in parallel with model processes. The actions are described in more detail later in the paper.

The processes are defined at a high level in order to be used as a model for different types of digital forensic investigations. We do not attempt to prescribe the exact details of each process. Many different

types of digital forensic investigations exist, such as live forensics, cloud forensics, network forensics and mobile phone forensics. The detailed procedures for each process should be defined for each specific type of digital forensic investigation. However, defining all these procedures is outside the scope of this paper. The proposed model should, therefore, be used as an "umbrella model" for the various types of digital forensic investigations. The detailed procedures are left to be implemented by other standards and by the digital forensic community.

3.3 Model Application Environment

We use a hypothetical banking environment to illustrate the harmonized model and its component processes. We assume that the four aims of digital forensic readiness must be achieved at a particular branch of a bank.

The information system at the bank branch has the following components:

- Two workstations (personal computers) that run a banking application. Access to the workstation operating system and the banking application uses single-factor, password-based authentication. The banking application is a web-based, thin-client application. An application log is stored locally on the client and centrally on the bank server.
- Two digital cameras that record the activities of employees at the workstations.
- Two digital cameras that record activities at the branch.
- One networked video recorder that records data from all four cameras.
- One switch that connects the workstations, cameras and networked video recorder in a local-area network (LAN).
- A router that connects the branch LAN to the bank's wide-area network (WAN).

Certain policies are defined for the information system. The policies specify how the system should function:

- Networked video recorder data is backed up and taken off-site once a day.
- Clients are identified manually by inspecting their identity documents (IDs). Each transaction at a bank counter is authorized by a

banking client's signature. The signature must be compared with the signature on the banking client's ID. The ID with the banking client's signature is scanned and archived in a central location.

3.4 Model Processes

This section describes the processes in the harmonized model along with their inputs and outputs.

Scenario Definition Process. This process involves the examination of all scenarios that may require digital evidence. The input to this process includes all the information regarding system architecture, system technology (hardware and software), policies, procedures and business processes. The input also includes the DFIRP aims. We refer to this set of inputs as "pre-known system inputs."

Similar inputs exist for all the other processes in the model. For example, the pre-known system inputs may include the network topology, specifications of models and hardware components, specifications of firmware, operating systems and applications for each piece of hardware, information security policies governing system use and the descriptions of the business use of the system to which the model is applied.

The output of this process is a set of scenario definitions. The scenarios may correspond to information security incidents such as the unauthorized use of resources. They may also correspond to events that require digital forensic investigations, such as the use of a computer to distribute child pornography.

During the scenario definition process, a risk assessment should be performed for each scenario separately. A risk assessment helps identify the possible threats, vulnerabilities and related scenarios where digital evidence might be required. Based on the assessed risk from certain threats, vulnerabilities or scenarios, the later processes can be used to better decide on the measures necessary to achieve forensic readiness, taking into account the risk levels, costs and benefits of the possible measures in order to reduce the identified risk. For example, a better decision can be made about the need to centrally collect and process all system log data in order to improve digital forensic readiness. In addition, the risk assessment would help determine the protection mechanisms needed for the centralized storage of log data, such as firewalls, link encryption, storage data encryption and change tracking.

An example scenario is the misuse of the banking application, where the application is used to steal credit card information. Another scenario is a complaint from a client claiming that he did not withdraw money from his account at the branch at a certain date.

The scenario definition process is a logical start for the DFIRP implementation because proper scenario analysis lays the foundation for all subsequent processes. After this initial process, it is necessary to specify all the possible sources of digital evidence based on the defined scenarios.

Source Identification Process. During this process, it is necessary to identify all the possible sources of digital evidence in the information system. Note that, for reasons of simplicity, inputs are represented as single arrows in Figure 1. The output of the process is the possible sources of evidence, e.g., registry files, temporary Internet files, email archives and application logs.

Some of the identified sources of evidence might not be available. For example, access logging may be not implemented in the information system. In such cases, methods for making the identified sources available and the use of alternative sources should be explored.

In our hypothetical information system, the possible sources of evidence based on the identified scenarios are:

- Data from the two workstations, especially banking application logs, temporary Internet files, text editor logs, email stored on the workstations, traces of deleted files and traces of modified files.
- Banking application logs stored at the bank's data center.
- Banking transaction data, such as signed transaction documents, stored at a central location.
- Video recordings from the networked video recorder.
- Backed-up data from the networked video recorder.

After the possible evidentiary sources have been identified, it is necessary to specify how these sources should be handled. This is accomplished using the planning pre-incident collection process and the planning pre-incident analysis process.

Planning Pre-Incident Collection Process. During this process, procedures are defined for pre-incident collection, storage and manipulation of data that represents possible digital evidence. Note that the data collection period is determined based on a risk assessment. For example, this could mean determining how often an organization would save the application log to a central repository to ensure the integrity of log data in the event that the application is compromised. The collection, storage and manipulation of data must conform to digital forensic principles

(e.g., chain of custody and evidence preservation) so that the digital evidence is admissible in a court of law. Also, the data retention period should be determined based on two factors: (i) risk assessment; and (ii) previous experience regarding incident detection, data quantity, network capacity and other matters that could influence the cost or efficiency of the process.

In the case of the hypothetical banking information system, the collection procedures for possible sources are:

- Collection of images of workstations is to be performed once a week. Images are to be stored off-site, securely and safely to preserve evidence. They are to be retained for a period of one year.

- Collection of banking application logs stored locally, temporary Internet files and text editors logs is to be performed daily. The data is to be sent via the network connection to the central repository. The data is to be retained for a period of five years.

- Deleting emails from the email server is forbidden. The emails are to be retained for a longer period of time, depending on the prevailing laws and regulations.

- Banking application logs and banking transactions data stored centrally are to be backed-up daily. Backed-up data is to be retained for a period of ten years.

- Video recordings from the networked video recorder are to be streamed to a central networked video recorder and retained for a period of two years.

- Backed-up data from the networked video recorder is to be retained for a period of two years.

- An intrusion prevention system is to be used to collect LAN network traffic data and traffic data to/from the WAN. This data is to be stored at a central location and retained for a period of one month.

Planning Pre-Incident Analysis Process. This process defines procedures for pre-incident analysis of data representing possible digital evidence. The aim of the analysis is to enable incident detection. Therefore, the procedures defined in this process must include exact information on how incidents are detected and the behavior that constitutes each incident.

The tasks of data analysis and incident detection are often outside the scope of target information systems (information systems that might come under a digital forensic investigation). Therefore, we recommend that this process defines an interface between the information system and a monitoring system that analyzes data in order to detect incidents.

In the case of our hypothetical banking information system, it would be necessary to have custom scripts or commercial software (e.g., for change tracking, intrusion detection and business intelligence) to analyze the information collected (both locally and centrally) in order to detect anomalies and possible incidents. Information security best practices should be taken into consideration as well as bank business processes and policies.

Planning Incident Detection Process. Since the main goal of the planning pre-incident analysis process is to enable incident detection, the next logical process is the planning incident detection process. The output of this process includes the actions to be performed after an incident is detected, especially collecting the information to be passed to the digital forensic investigation process. The information should also include pre-known system inputs, results from all DFIRP processes and data gathered and generated during the implementation process.

In the case of our hypothetical banking information system, when an incident is detected via pre-incident analysis, the information gathered by relevant software (e.g., for change tracking, intrusion detection and business intelligence) should be automatically sent to the bank's central information system and should trigger incident response activities.

Architecture Definition Process. This process involves the definition of an information system architecture for the information system that is to be forensic ready. The process draws on the results of all the previous processes. The process is introduced in order to implement better forensic readiness by taking into account all relevant matters when redefining the system architecture. The aim is to customize the system architecture to accommodate the four DFIRP aims.

In the case of our hypothetical information system, the architecture definition would include decisions to store no application data locally, to introduce automated document reading and biometric identification to verify customer identity, and to introduce three-factor authentication for workstations and applications (e.g., PINs, biometrics and smart cards).

Implementation Processes Group. This group implements the results of all the previous processes. Although the processes compris-

ing this group are distinctive, they are presented in one section, unlike the other processes that are presented separately. This is because all the processes in the implementation processes group are concerned with the implementation of results from the planning processes group. All these processes represent the implementation of technical or non-technical measures defined in the other processes.

In practice, the measures defined in the architecture definition process should be implemented. This is followed by the pre-incident collection, pre-incident analysis and incident detection processes.

A clear difference exists between the processes in the implementation processes group (Figure 2) and the processes in the planning processes group. The difference is that, for example, the process listed as implementing pre-incident collection in the planning processes group is tasked with defining what data is collected and how it is collected; on the other hand, the implementing pre-incident collection process of the implementation processes group is tasked with implementing the results of the implementing pre-incident collection process, including digital evidence collection.

It is important that the roles of the various people in the system are considered. People represent users. However, people are also custodians and owners of information system components. The procedures must include relevant information for all the people involved with the system. Also, training and awareness sessions must be conducted for all people involved with the information system.

The output of the implementation processes group is an information system that is finally forensically ready. This process represents an interface to the DFIP; in fact, it straddles the tasks of readiness and investigation.

Assessment of Implementation Process. After forensic readiness been implemented, it is necessary to start the assessment process. This process examines the results of the implementation of forensic readiness to determine if it conforms to the DFIRP aims.

During this process, a legal revision should be carried out for all procedures, measures and architectures defined when implementing the model. The revision should show whether or not there is conformity with the legal environment and digital forensic principles in order to ensure evidence admissibility.

In the case of our hypothetical banking information system, the assessment process would take the form of an internal audit or external audit. The goals of the audit would be to check if the implementation

conforms to the results of the planning processes group and the four DFIRP aims.

Implementation of Assessment Results Process. This process is concerned with implementing the conclusions from the previous process. The process is optional because it is possible that no actions are needed based on the results of the assessment of implementation process.

During this process, it is necessary to decide on recommendations for changes in one or more of the previous processes. The main decision here is whether to go back to one of the planning processes or to go back to an implementation process based on the results of the implementation assessment process.

3.5 Parallel Actions

This section discusses the actions that must run in parallel with the processes. The parallel actions are defined as the principles that should be translated into actions in the DFIRP. Examples are the principle that evidentiary integrity must be preserved throughout the process and that the chain of evidence must be preserved. These principles are found in existing DFIP models [9–11].

The parallel actions in the DFIRP model are: preserving the chain of evidence, preserving evidence, defining information flow, documentation and obtaining authorization (Figure 2). These actions are implementations of well-established principles of digital forensics.

The actions run in parallel with all the other processes to ensure the admissibility of digital evidence. Parallel actions also enhance the efficiency of an investigation. Some actions defined by other researchers, such as obtaining authorization and preparing documentation, run across several processes.

Preserving the Chain of Evidence. All legal requirements must be complied with and all actions involving digital evidence must be properly documented in order to preserve the chain of evidence and the integrity of evidence. This principle must be followed throughout the DFIRP.

Preserving Evidence. The integrity of the original digital evidence must be preserved. This is achieved using strict procedures from the time that the incident is detected to the time that the investigation is closed. The procedures must ensure that the original evidence is not changed and, even more importantly, they must guarantee that no opportunity for evidence tampering arises during the entire investigation.

Information Flow. It is important to identify and describe all information flows so that they can be supported and protected. An example information flow is the exchange of digital evidence between two investigators. This information flow could be protected using a public key infrastructure to preserve confidentiality, timestamping to identify the different investigators, and authenticating the evidence to protect its integrity.

A defined information flow should exist between each of the processes and between the various stakeholders, including investigators, managers and external organizations. For example, there should be defined information flows between investigators and managers of the information system being investigated, including obtaining authorizations from the managers (system owners or system custodians), and informing managers about security incidents, their possible consequences and the required actions.

Documentation. Every action performed should be documented to preserve the chain of evidence, and to increase efficiency, resource utilization and the likelihood of a successful investigation. This would, for example, include documenting how the information obtained during pre-incident collection has been stored and processed, along with all the persons who have had access to the information.

Obtaining Authorization. Proper authorization should be obtained for every action that is performed. Depending on the action, the authorization may have to come from government entities, system owners, system custodians and/or principals.

4. Conclusions

The proposed model harmonizes existing efforts related to DFIRP models. It has a broader scope than digital forensic readiness processes and existing digital forensic process models. The broader scope is manifested by the definition of additional processes such as the planning pre-incident data analysis process, architecture definition process and assessment processes.

The processes in the harmonized model are well-defined in terms of scope and functions. The processes deal with all the matters covered by existing models as well as matters that are outside the scope of existing models, such as customizing the architecture definition of a target information system to achieve the digital forensic readiness goals. In fact, customizing the architecture definition is a novel concept that contributes to a more holistic approach to digital forensic readiness.

Another novel concept is the incorporation of actions based on digital forensic principles that are performed in parallel with processes in the harmonized model. These parallel actions enhance the efficiency of investigations and ensure the admissibility of digital evidence.

Using the harmonized DFIRP model provides several benefits. These include improved admissibility of digital evidence, reduced human errors and omissions during the DFIRP, and better resource utilization when implementing digital forensic readiness and conducting digital forensic investigations. Also, the harmonized DFIRP model can improve the overall security of an information system by raising awareness about specific incidents and alternative scenarios.

Our future work will apply the harmonized model to a functional system and measure its conformance with the four DFIRP aims, both before and after the implementation. Future work will also involve defining an interface between the harmonized DFIRP model and a DFIP model to achieve a holistic and harmonized DFIP model. Initial work related to these topics and others is discussed in [5].

References

[1] N. Beebe and J. Clark, A hierarchical, objectives-based framework for the digital investigations process, *Digital Investigation*, vol. 2(2), pp. 146–166, 2005.

[2] B. Carrier and E. Spafford, Getting physical with the digital investigation process, *International Journal of Digital Evidence*, vol. 2(2), 2003.

[3] B. Carrier and E. Spafford, An event-based digital forensic investigation framework, *Proceedings of the Fourth Digital Forensics Research Workshop*, 2004.

[4] International Standards Organization and International Electrotechnical Commission, ISO/IEC 12207, Systems and Software Engineering – Software Life Cycle Processes, Geneva, Switzerland, 2008.

[5] International Standards Organization and International Electrotechnical Commission, ISO/IEC 27043 – Information Technology – Security Techniques – Digital Evidence Investigation Principles and Processes (Draft), Geneva, Switzerland, 2012.

[6] K. Mandia, C. Prosise and M. Pepe, *Incident Response and Computer Forensics*, McGraw-Hill/Osborne, Emeryville, California, 2003.

[7] Y. Manzano and A. Yasinsac, Policies to enhance computer and network forensics, *Proceedings of the Second Annual IEEE SMC Information Assurance Workshop*, pp. 289–295, 2001.

[8] G. Palmer, A Road Map for Digital Forensic Research, DFRWS Technical Report DTR-T001-01 Final, Digital Forensic Research Workshop, Utica, New York (`www.dfrws.org/2001/dfrws-rm-final.pdf`), 2001.

[9] R. Rowlingson, A ten step process for forensic readiness, *International Journal of Digital Evidence*, vol. 2(3), 2004.

[10] J. Tan, Forensic readiness: Strategic thinking on incident response, presented at the *Second Annual CanSecWest Conference*, 2001.

[11] A. Valjarevic and H. Venter, Harmonized digital forensic investigation process model, *Proceedings of Eleventh Annual South African Information Security Conference*, 2012.

[12] J. Wolfe-Wilson and H. Wolfe, Management strategies for implementing forensic security measures, *Information Security Technical Report*, vol. 8(2), pp. 55–64, 2003.