Towards a Prototype for Guidance and Implementation of a Standardized Digital Forensic Investigation Process

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

Melissa Ingles
Department of Computer Science,
University of Pretoria
Pretoria, South Africa

***Abstract*—Performing a digital forensic investigation requires a standardized and formalized process to be followed. There currently is neither an international standard formalizing such process nor does a global, harmonized digital forensic investigation process exist. Further, there exists no application that would guide a digital forensic investigator to efficiently implement such a process. This paper proposes the implementation of such a prototype in order to cater for this need. A comprehensive and harmonized digital forensic investigation process model has been proposed by the authors in their previous work and this model is used as a basis of the prototype. The prototype is in the form of a software application which would have two main functionalities. The first functionality would be to act as an expert system that can be used for guidance and training of novice investigators. The second functionality would be to enable reliable logging of all actions taken within the processes proposed in a comprehensive and harmonized digital forensic investigation process model. Ultimately, the latter functionality would enable the validation of use of a proper process. The benefits of such prototype include possible improvement in efficiency and effectiveness of an investigation due to the fact that clear guidelines will be provided when following the process for the course of the investigation. Another benefit includes easier training of novice investigators. The last, and possibly most important benefit, includes that higher admissibility of digital evidence as well as results and conclusions of digital forensic investigations will be possible due to the fact that it will be easier to show that the correct standardized process was followed.**

Keywords- implementation prototype, digital forensics, digital forensic investigation process model, harmonization, standardization, ISO/IEC 27043

I. INTRODUCTION

Dealing with digital evidence requires a standardized and formalized process in order for digital evidence to be accepted in a court of law [1].

Methods and process models for the digital forensic investigation process have been – more often than not – developed mostly by practitioners and digital forensic investigators based on personal experience and expertise, on an ad hoc bases, without the main aim to reach harmonization and standardization within the field. In the past decade, there were also a number of academic research projects conducted in order to establish a digital forensic investigation process model.

By the time of writing this paper, there currently exists no international standard formalizing the digital forensic investigation process. An effort to standardize the process is, however, in an advanced stage within the International Standardization Organization (ISO) as a result of this research [2]. The standard is currently in final draft international standard status and it is expected that it will come into effect by the end of 2014.

Further, there is no appropriate prototype or software application that would guide one through the implementation of a standardized and harmonized digital forensic investigation process. In their previous work, the authors proposed a comprehensive and harmonized digital forensic investigation process model [3,4]. The benefits of the use of such a prototype are discussed later in the paper.

The remainder of the paper is structured as follows. Section 2 provides background on digital forensics, past work on the digital forensic investigation process and the comprehensive and harmonized digital forensic investigation process model proposed by the authors in their previous work [3,4]. After that, Section 3 presents the proposed prototype. Section 4 concentrates on discussing the proposed prototype and its potential use and benefits. Section 5 concludes this paper and gives indications of future work.

II. BACKGROUND

The subsections to follow provide background on the following topics. First, background on digital forensics investigation readiness is provided in order to introduce the reader to the basics of the subject. After that, we provide background on past work on the digital forensic investigation process. Last, but not least, we provide background on the comprehensive and harmonized digital forensic investigation process model proposed by the authors in their previous work [3,4]. This process model represents the basis of the prototype

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

proposed in this paper and is, therefore, explained here, although at a high level only due to space constraints.

A. Digital Forensics

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

B. Related Work on the Digital Forensic Investigation Process Models

Many digital forensic investigation process models have been proposed across the world, however, there exist numerous disparities among these process models. To illustrate this point, the remainder of this section elaborates on the various process models.

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 [5], the need for a standard framework for digital forensics has been widely acknowledged [6-12]. The digital forensic investigation process model proposed at this workshop includes the following seven processes: Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision. The process model was defined as iterative. Reith, Carr and Gunsch [6] proposed a digital forensic investigation process model known as the abstract model, which includes the following processes: identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning evidence.

The U.S. Department of Justice (DOJ) published a process model in the Electronic Crime Scene Investigation Guide aimed at first responders [7]. This proposed process model includes the following processes: preparation, recognition and identification, documentation of the crime scene, collection and preservation, packaging and transportation, examination, analysis and reporting.

Carrier and Spafford [8] propose a process model based on the following requirements: The model must be based on existing theory for physical crime investigations; The model must be practical and follow the same steps that an actual investigation would take; The model must be general with respect to technology and not be constrained to current products and procedures; The model must be specific enough that general technology requirements for each process can be developed; The model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response. The model proposed by Carrier and Spafford [8] includes 17 processes organized into the following five groups: readiness processes, deployment processes, physical crime scene investigation processes, digital crime scene investigation processes and review process. Carrier and Spafford [9] also proposed another (similar) event-based process model. This model is, again, based on physical crime investigation and it is suggested that digital crime scene investigation should occur as a subset of a physical crime scene investigation. The paper concentrates on digital crime scene investigation processes and how to find the causes and effects of events during a digital forensic investigation.

Mandia, Prosise and Pepe [10] proposed a digital forensic investigation process known as the incident model, which contains the following processes: pre-incident preparation, detection of the incident, initial response, response strategy formulation, duplication (system backup), investigation, secure measure implementation (isolation and containing the suspect system), network monitoring, recovery (recovery of the suspect system to original process), reporting and follow-up.

Beebe and Clark [11] proposed a hierarchical, objectives-based digital forensic investigation process model and also drew a comprehensive comparison between their proposed process model and previous works in this field. The model they proposed is multi-tiered, which constitutes a novel approach. First-tier processes proposed in [11] include the following: preparation, incident response, data collection, data analysis, findings presentation and closure. In their opinion, second-tier sub-processes should be defined in such a way that these are inclusive of all possible types of crime and types of digital evidence.

Cuardhuáin [12] proposed an extended and comprehensive model of cybercrime investigations, which is very comprehensive. The harmonized model also includes information flow description between different processes.

Casey and Rose [13] define processes of digital forensic investigation process as: gather information and make observations, form a hypothesis to explain observations, evaluate the hypothesis, draw conclusions and communicate findings.

Cohen [14] proposed a process model that includes the following processes: identification, collection, preservation, transportation, storage, analysis, interpretation, attribution, reconstruction, presentation and destruction. Cohen, Lowrie and Preston [15] discuss the state of the science of digital evidence examination and consensus in digital evidence examination. He recognizes that numerous calls have been made for scientific approaches and formal methods in the field of digital forensics.

In the United Kingdom, examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and integrity of evidence [16]. These guidelines do not explicitly set out the digital forensic investigation process model, but, through recommendations, the given process model can be constructed, containing following processes: preparations for investigation, crime scene group of processes, secure and control the crime scene, photograph and document the scene, initial collecting of

volatile data, attaching exhibit labels, documenting each action performed, transportation, storage, evidence recovery group of processes, the collection process, the examination process, the analyses process, the reporting process, disclosure.

Based on related work on the digital forensic investigation process, the authors of this paper concluded that there are significant disparities among existing digital forensic investigation process models. Disparities pertain to the number of processes included, the scope of models, and the scope of similarly-named processes within different models, the hierarchy levels and even concepts applied to the construction of the model (i.e. some of the models are based on the physical crime investigation processes).

An effort to standardize the process is, however, in an advanced state within the International Standardization Organization (ISO) as mentioned before [2]. This international standard provides guidelines that encapsulate and harmonize these models for common investigation processes across various investigation scenarios [2].

C. Standardized Digital Forensic Investigation Process: A Comprehensive and Harmonized Digital Forensic Investigation Process

In this section the authors present an overview of their previously proposed work, namely the comprehensive and harmonized digital forensic investigation process model [3,4]. Ultimately, once the proposed international standard [2] has been published, this will officially become a standardized, internationally accepted process.

Here we present an extrapolated overview at a high level in order for the reader to familiarize him/her with the model. The aim of this section is not to explain the details for the specific processes within the model.

The digital investigation process model consists of several processes. Each of these processes are generic enough and proposed at such a level of abstraction so that they can be used for different types of digital forensic investigation scenarios and for different types of digital evidence. The model proposes a harmonized organization of the processes while introducing a novel approach in the way some of the processes have been implemented, i.e., *concurrent processes*. The authors define concurrent processes as the principle actions which should be achieved in parallel with other processes within the digital forensic investigation process model.

In order to abstract all processes on a higher level, all digital forensic investigation processes in the harmonized model are categorized into the following digital forensic investigation process classes [2]: Readiness processes class, Initialization processes class, Acquisitive processes class, Investigative processes class and Concurrent processes class.

Following is an overview of the proposed classes. The aim of this overview is to enable the reader to gain a holistic, high-level view of the model and its classes, without going into details of each individual processes.

The readiness class of processes deals with pre-incident investigation processes aimed at reaching digital forensic investigation readiness within an organization. The processes in this class attempt to maximize the use of potential digital evidence, while minimizing the costs and interference with business processes. This class of processes should also enable preserving or improving the information security of potential digital evidence. Note that the readiness processes are optional to the rest of the digital forensic investigation processes.

The next three classes include the *initialization processes*, *acquisitive processes and investigative processes* respectively. All these classes follow one another and do not overlap in time. As shown in Figure 1, however, the *concurrent processes* class runs in parallel with all other classes, ensuring the application of digital forensics principles.

The initialization class of processes deals with the initial commencement of the digital forensic investigation. The processes in this class are concerned with incident detection, first response, planning and preparation of the actual digital forensic investigation. These processes are of extreme importance for the success and effectiveness of the investigation, as these represent the basics and foundation for any of the processes following the initialization processes. If any error or omission is made during these processes digital evidence might become unusable or unavailable and complete process integrity might be endangered.

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

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

Figure 1 shows the classes of digital forensic investigation processes and an overview of their relations.

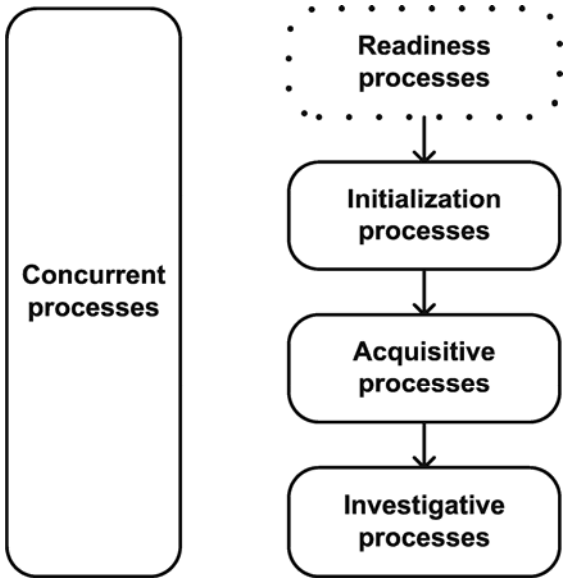

Figure 1: The classes of the standardized digital forensic investigation process model

Figure 2 shows the detailed process of the standardized model. The figure is given in order for reader to gain limited insight of individual processes within the main process classes, without expanding on details, as explained before.

III. Prototype for Guidance and Implementation of a Standardized Digital Forensic Investigation Process

This section explains the proposed prototype, its potential use and benefits.

The prototype is in the form of a software application which has two main functionalities. The first main functionality would be to act as an expert system that can be used for guidance and training of novice investigators. The second main functionality would be to enable the implementation of the investigation process while reliably logging all actions in a digital forensic fashion. Ultimately, the latter functionality would enable the validation of use of a proper digital forensic investigation process.

The use of the proposed software (prototype) would significantly help any organization involved with digital forensic investigations to follow a standardized process and improve admissibility of digital evidence and results of investigations. Also, the software can be used by organizations involved with or providing training in the field.

For illustration purposes only, Figure 3 presents a screenshot of the Graphical User Interface showing the readiness processes class and in the specific scenario definition process. It is intended that one can follow the processes, as per the standardized process model [2], while the software provides guidance (on the left side of the user pane) and possibility to implement the process (on the right side of the pane). While only accessing the guidance portion, the user can freely browse through processes for information purposes, but when execution of the process has started, the user is forced to follow the standardized process sequence.

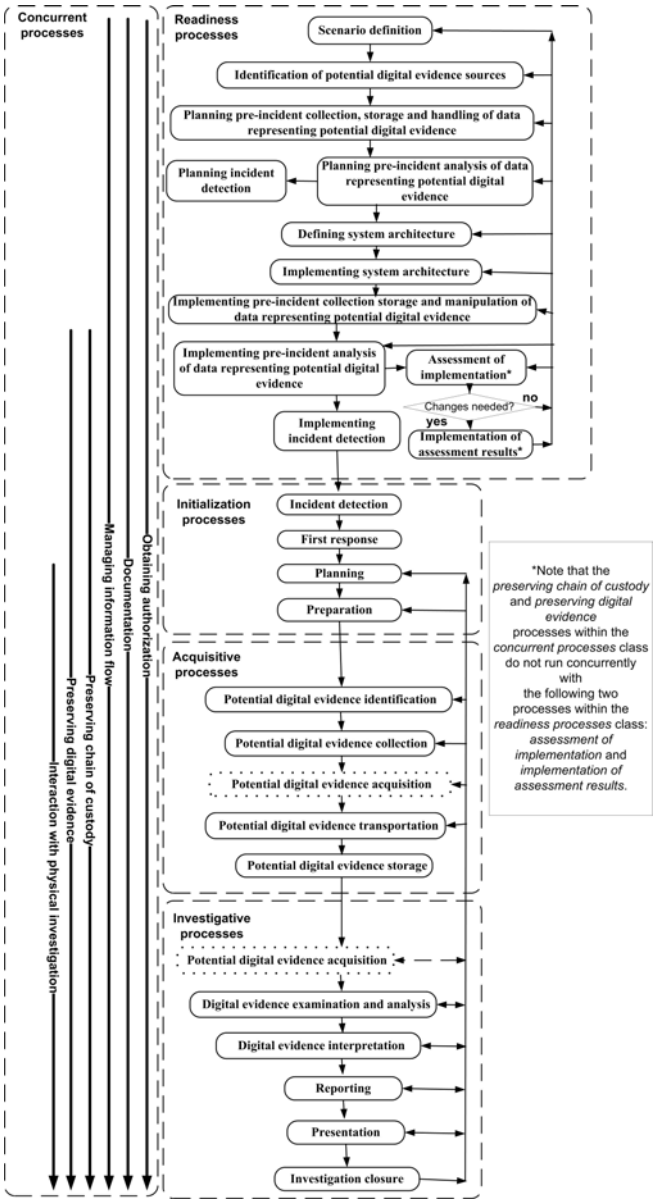

Figure 2: Standardized digital forensic investigation process model

The user can also choose to generate reports through selecting the “Reports” tab from the task bar at the top.

The information system security is based on the use of cryptographic technologies in order to ensure efficient access control, confidentiality and integrity of all information.

Non-repudiation of user actions is enabled through use of digital signatures. This also enables to verify the authenticity of actions and any associated information (files) as accessed by the user.

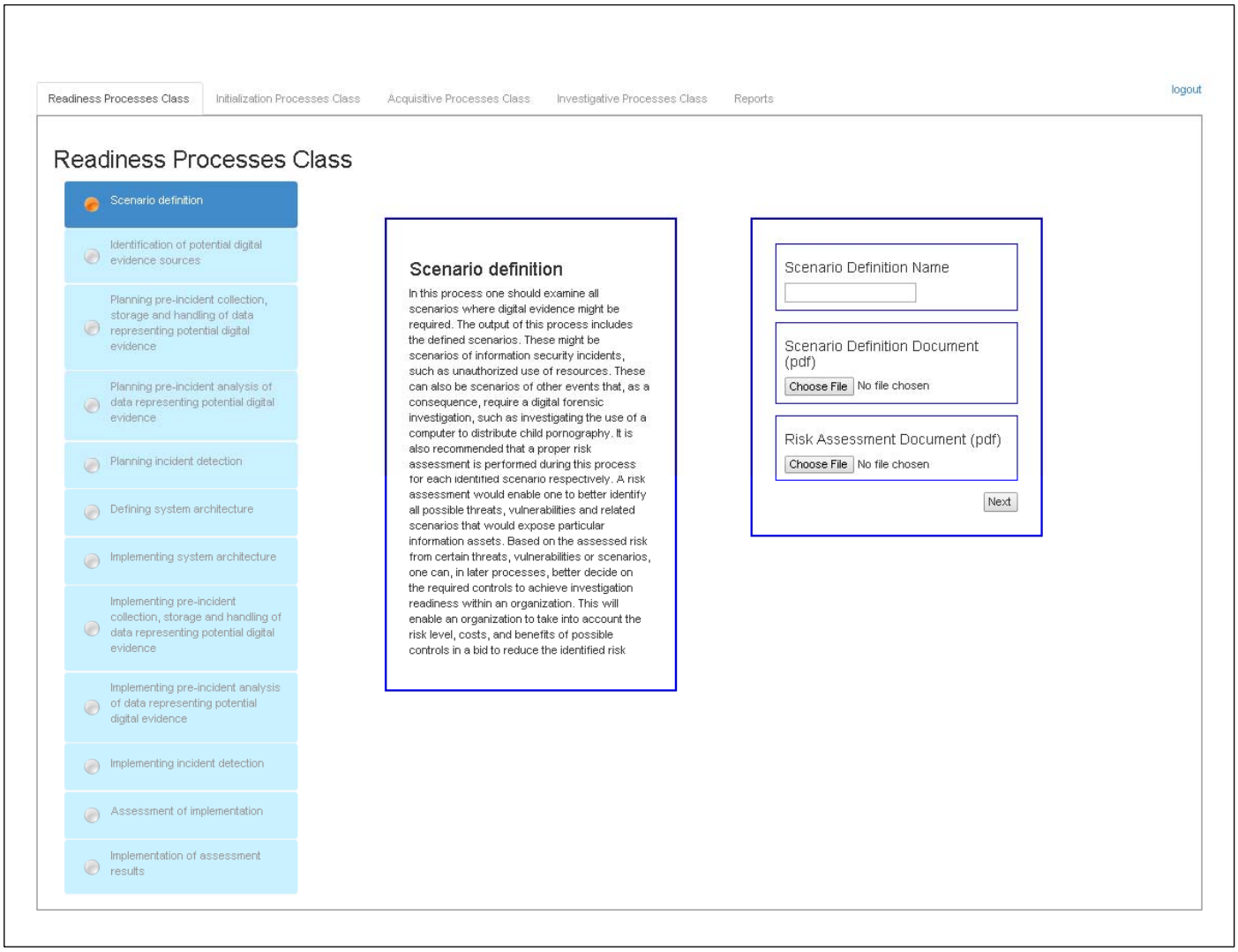

Figure 3: Screenshot of the Graphical User Interface: Readiness processes class - Scenario definition process

The software includes comprehensive reporting per project (specific digital forensic investigation), timeline, action and user. Especially, reporting is provided per concurrent processes in order to enable one to verify implementation of these processes that, among other things, ensure integrity of digital evidence and ensure the following of appropriate procedures for flow of information.

Access control is implemented as role based and it is based on the use of digital certificates.

The following sections explain the system layout, including the following:

- system architecture,
- components, and
- information system security.

A. System Architecture

This section gives an overview of the system architecture, with the focus on technology components used to realize the prototype (software).

Database – The database is implemented using MySQL which was chosen because it is free, fast and cross-platform. MySQL includes data security layers to protect data from intruders, passwords are encrypted and rights can be set up to allow only certain access.

Platform – The platform chosen for the prototype is web-based as this allows ease of use across multiple platforms and from any location. It enables collaboration of multiple users, from multiple organizations and even from multiple jurisdictions and countries. It is also better to provide the prototype as a Software as a Service (SaaS) because the user has no control over the server thus it can be optimized for complete security by the owner. Also SaaS can provide better cost effectiveness for the user and it enables user to concentrate on core activity- the digital forensic investigation.

Language and Framework – The prototype is implemented using the PHP coding language and the Laravel Framework. Laravel is a free, open source PHP web application framework, designed for the development of MVC (Model-View-Controller) web applications. The Laravel framework was chosen because of its MVC and REST (Representational state transfer) capabilities, as well as its database support and available add-ons and libraries. Laravel also has a number of important security related functionality such as encryption and authentication.

User management – For user management Sentry is used. Sentry is an add-on to Laravel that provides configurable authentication, authorization, user activation, groups and group permissions, login throttling, user suspension, user banning and it is interface driven. Sentry also encrypts all passwords and allows an easy way to authenticate a user and to prevent access to pages based on the user that is logged in.

Report generator – For generating reports DOMPDF is used. DOMPDF is an easy to use HTML to PDF converter and allows any styles that HTML can handle to be added to a PDF.

Component communication architecture – All components (see next section) communicate using RESTful services.

The next section concentrates on the functional components of the prototype.

B. Components

This section describes functional components of the prototype and their interaction.

Guidance module – This module provides guidance to the user in terms of how the process should be implemented – though either graphical or textual advice, or both. This component is optional to the user. The user can choose to go through this module or not, depending on whether he needs the guidance or not. The guidance module is especially intended for use by novice investigators or other novice professionals involved with digital forensic investigation.

Process Implementation and Logging module – This module guides the user through completing the processes, it allows the user to choose a process, and upload the documents for the process. Once the user uploads the data for this process (this can be in the form of text and/or files and it can also be in form of predefined forms populated with user data) the data will get passed through the Encryption module and then through the Digital signature module. These modules will be explained next. After the data passed through these modules, the encrypted and digitally signed text data will be saved to the database and the encrypted and signed documents will be saved to the disk of the server. The action the user preformed, along with the data and other relevant information, will then be logged to the database and the user will be able to select a new process to implement (as per the standardized process) or choose to generate a report. In actual fact the user will be able to choose to generate report at any point of work in Process Implementation and Logging Module.

Encryption module – The encryption module is responsible for encryption of all textual data entered by the user as well as any files uploaded by the user. The data is encrypted in such a manner that only authorized users can access it.

Digital Signatures for actions and information module – When the user preforms an action (uploads data or enters text in predefined forms) or generates a report all textual data and documents are digitally signed using users digital signing private key. The digital signing takes place on the client-side of the proposed software because the user's digital signing private key is private to the user and cannot be stored on the server.

User Management and Access Control module – This module is responsible for managing user authentication and access control. Access control is role based. Only users with the correct roles are allowed to access certain projects, data and functionalities of the software.

Reporting module – This module is responsible for generating reports of users' actions. Reporting module is of crucial importance as it enables verification of following a proper standardized process and adhering to all guidelines and requirements. This module will enable creation of reports by authorized users, per project, user, timeline, and action (process).

The next sub section explains the sequence of action within the prototype (software) and interactions between the components.

C. Activity diagram

Figure 4 represents prototype component activity diagram. This diagram shows interaction between the components and sequence of actions within the prototype.

Following is an explanation of the activity diagram. The activity within the prototype software starts with the user accessing the website of the prototype. If user is not logged in, he/she is redirected to the login page, where he/she can log in and the system will authenticate his/her credentials. If the user is logged in, his/her roles will be checked to see if he/she has permission to access the page he/she is trying to access. If he/she does not have permission, he/she will get an error and will have to retry. If he/she does have permission the, start page will be loaded.

The user can then choose whether he/she wants to follow a process, make a report or log out.

If the user chooses to make a report, he/she will be shown the reporting page. The user will then be able to choose the report he/she wants to generate by clicking on appropriate report. The system will generate the report, use the user's digital certificate to sign the report and save the report to the disk. The user will then be able to choose whether he/she wants to print the report or save it to disk. After either of these steps, the user will be able to choose whether he/she again wants to follow a process, make a report or log out from the prototype.

If the user chooses to follow a process, he/she will be able to select the process he/she wants to view. The user will then be able to choose whether he/she wants to print the process, see guidance for the process or continue with the execution of the process.

Printing the process would actually enable printing guidance or parts of guidance for the particular step.

If the user chooses guidance, he/she will see image and text data to guide him/her in executing the process. After that, he/she will be able to continue to follow the process.

When executing the process, the user can input the data requested by the process and upload any necessary files. The system will encrypt and digitally sign both the user data entered into predefined forms as well as the files that were uploaded. The encrypted and signed files will be saved to the disk. The encrypted and signed data entered by the user will be saved to a database.

The process name, date, user name, description of all activities and any other relevant information will be logged to the database for audit purposes.

The user will be able to choose again whether he/she wants to follow a new process, make a report or logout.

If the user logs out, he/she will be redirected to the logon page and the process will start over.

The next section is dedicated to the implementation of the information systems security.

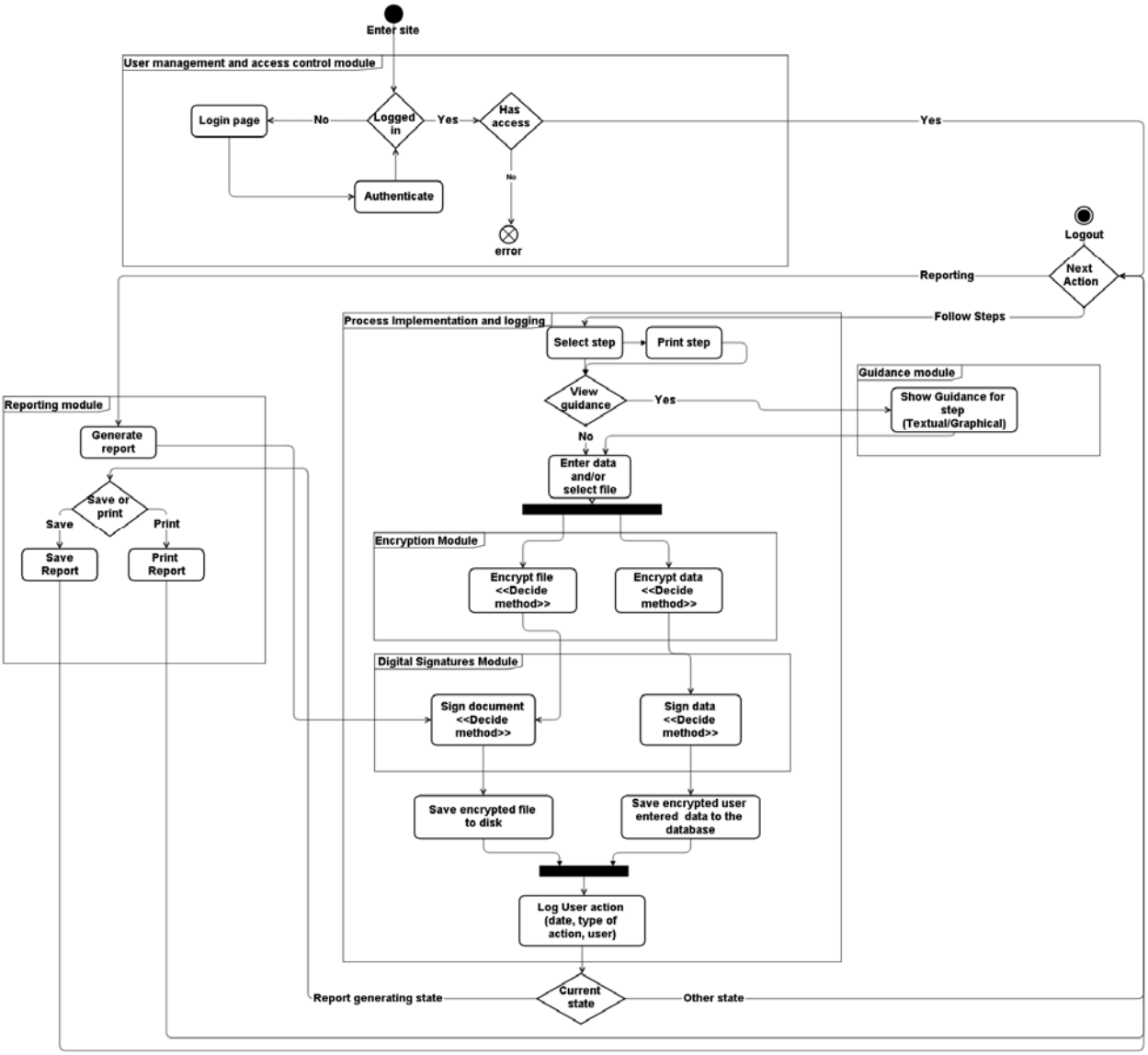

Figure 4: Prototype component activity diagram

D. *Information System Security*

This section explains basics of information systems security of the proposed software.

The system implements encryption of user files and data using AES256 (Advanced Encryption Standard 256) algorithm as well as digital signing to ensure the integrity and confidentiality of all data.

All connections to the server are encrypted through a HTTPS using either SSL 3 (Secure Socket Layer 3) or any version of TLS (Transport Layer Security) protocols based on what the user's browser supports. If the browser does not support either of these two protocols the user will be asked to first upgrade his browser.

IV. DISCUSSION

The proposed prototype enables one to easily follow the standardized process, which would result in higher admissibility of digital evidence and results of digital forensic investigations. Higher admissibility of digital evidence and results of digital forensic investigations would be possible due to the fact that courts of law would probably be more satisfied that a standardized and formalized process was followed during a digital forensic investigation, which passed significant peer review and was ultimately accepted as an international standard.

Another use of such a prototype is that it would provide for training of novice investigators. Yet another benefit is the possible improvement in efficiency and effectiveness of digital forensic investigations due to the fact that clear process guidelines are available.

These two main functionalities that provide the benefits as explained above, are acting as an expert system that can be used for guidance and training of novice investigators and enabling the implementation of the investigation process while reliably logging all actions in a digital forensic fashion.

The authors proposed a well-defined architecture for the prototype and defined key functional components, while taking into consideration information systems security. A web-based platform was chosen to develop the prototype in order to cater for multiple users from multiple locations and jurisdictions, with minimal requirements for client infrastructure. Cryptography is used to ensure confidentiality and integrity of all information, as well as to ensure non-repudiation of user actions.

The next section concludes the paper.

V. CONCLUSION

The problem that this paper addressed is that there exists, by the time of writing this paper, no prototype or software application for guidance through and implementation of a standardized digital forensic investigation process model that can be used as a standardized tool.

The proposed prototype addresses the problem by being a tool that can help one to properly follow a standardized digital forensic investigation process.

The authors believe that the proposed prototype is a significant step towards enabling implementation of a standardized digital forensic investigation process model. The proposed prototype not only enables implementation but also logging and non-repudiation of all user activities, with special concentration on concurrent processes, which cater for evidence integrity.

Future work will include further development of the prototype in the form of software application. Implementation of such a prototype will enable evaluating and testing the proposed process model [3,4] and its effectiveness.

ACKNOWLEDGEMENT

This work is based on the research supported in part by the National Research Foundation of South Africa (Grant Numbers 88211, 89143 and TP13081227420.

REFERENCES

[1] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 1993

[2] ISO/IEC 27043, "Information technology — Security techniques — Investigation principles and processes", unpublished final draft international standard, 2014

[3] Valjarevic and Venter, "Harmonized digital forensic investigation process model", Proceedings of Information Security South Africa 2012 Conference, 2012

[4] Valjarevic and Venter, "Towards a harmonized digital forensic investigation readiness process model", Proceedings of Ninth Annual IFIP WG 11.9 Conference, 2013

[5] Palmer, "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

[6] Reith, Carr and Gunsch, "An examination of digital forensic models", International Journal of Digital Evidence, 2002

[7] DOJ, The U.S. Department of Justice , "Electronic crime scene investigation- a guide for first responders", 2001

[8] Carrier and Spafford, "Getting physical with the digital investigation process", International Journal of Digital Evidence, Vol. 2, 2, [Electronic version], 2003

[9] Carrier and Spafford, "An event-based digital forensic investigation framework", Digital Investigation 2(2), 2005

[10] Mandia, Prosise and Pepe, "Incident response & computer forensics" (Second Ed.), McGraw-Hill/Osborne, Emeryville, 2003

[11] Beebe and Clark, "A hierarchical, objectives-based framework for the digital investigations process", Digital Investigation 2(2), 2005

[12] Cuardhuain, "An extended model of cybercrime investigations", International Journal of Digital Evidence, summer 2004, Volume 3, Issue 1, 2004

[13] Casey and Rose, chapter "Forensic analysis " in "Handbook of digital forensics and investigation", 2010, pp. 21-62

[14] Cohen, "Fundamentals of digital forensic evidence, chapter in handbook of information and communication security", accessed at all.net on 04.01.2011, 2011

[15] Cohen, Lowrie and Preston, "The state of the science of digital evidence examination", 2011

[16] ACPO, "ACPO good practice guide for computer-based evidence", http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf, last accessed 18.02.2013, 2008