International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:11, No:3, 2017

A Method to Enhance the Accuracy of Digital Forensic in the Absence of Sufficient Evidence in Saudi Arabia

Fahad Alanazi, Andrew Jones

***Abstract*—**Digital forensics seeks to achieve the successful investigation of digital crimes through obtaining acceptable evidence from digital devices that can be presented in a court of law. Thus, the digital forensics investigation is normally performed through a number of phases in order to achieve the required level of accuracy in the investigation processes. Since 1984 there have been a number of models and frameworks developed to support the digital investigation processes. In this paper, we review a number of the investigation processes that have been produced throughout the years and introduce a proposed digital forensic model which is based on the scope of the Saudi Arabia investigation process. The proposed model has been integrated with existing models for the investigation processes and produced a new phase to deal with a situation where there is initially insufficient evidence.

***Keywords*—**Digital forensics, Process, Metadata, Traceback, Saudi Arabia.

I. Introduction

THE digital investigation processes are basically the procedure which allows the outcomes of investigation into incidents of inappropriate behaviours and illegal and criminal activities to be of a quality which can be submitted to a court of law [8]. There are many digital investigation models and frameworks for procedures which have been developed around the world during the past three decades [6]. The digital investigation processes should follow a number of steps to achieve a successful outcome to a digital forensics investigation [8]. The models or frameworks are used by organisations to enhance their investigation procedures to ensure that evidence for presentation in the court is of an acceptable standard [6]. Thus, since early as 1984, law enforcement agencies, such as the FBI laboratory, made efforts to enhance the processes of digital investigations [18]. To avoid the risk of inadmissibility of the evidence which is the outcome of a digital investigation in the court, appropriate investigative processes need to be followed. Based on our observations, there are a number of digital investigation processes and frameworks that have been proposed, some of which tend to be applied to the wider environment and others applied to specific scenarios.

Fahad Alanazi is a post graduate student at De Montfort University, where he is currently studying for his PhD. (e-mail: fahad3n@hotmail.com).

Andy Jones is the Director of the Cyber Security Centre at the University of Hertfordshire and a visiting Professor at Edith Cowan University (e-mail: a.jones26@herts.ac.uk)

In this study, we integrate the available models and common phases of the investigation process to create a comprehensive model for the digital investigation process that can be applied to any scenario in Saudi Arabia, together with an additional phase which is called Traceback that is proposed to deal with situations where there is initially insufficient evidence.

II. Research Methodology

The proposed model uses the Grounded theory method which was developed by [12].

In this research, grounded theory is adopted for exploring and investigating the participants "views, opinions and perspectives" concerning the adoption of a method of a digital forensics investigation process in the absence of complete evidence in the Saudi Arabian context as the research method for a number of reasons: 1. The use of grounded theory is possible for this research because it is of an interpretive nature. 2. It is helpful for the researcher to build a theoretical framework which explains the data that was collected; this is because grounded theory includes systematic inductive methods for collecting and analysing data [12] to provide rigorous understanding into an unknown area relative to the researcher. 3. It is a useful method for assisting the researcher to create a model with which to identify the effects of a number of factors on Digital Forensics (DF) in the Saudi Arabian context. 4. It allows for the researcher to develop theory through generation of concepts and categories. 5. It is flexible and allows the researcher to update interview questions for identifying emergent and new issues. 6. Grounded theory differs from other research approaches through a constant interaction between the stages of data collection and analysis of data [17].

The data collection method that followed in this research was semi-structured interviews; it is to enable the participants to express their visions, concerns, opinions and feelings related to factors that impact the adoption of DF in the absence of sufficient evidence in Saudi Arabia.

This study follows the procedures for coding in accordance with Strauss' approach to emerge as the core category of the proposed model from data via three stages, namely open coding, axial coding and selective coding.

After examining the data and the relationships between the categories in the dimensions and properties and axial coding diagram, the core category of the digital investigation process in the absence of sufficient evidence has emerged.

III. Related Work on Digital Investigation Processes

Digital forensics investigations in Saudi Arabia follow a procedure that is used by the investigators to identify the suspect and relevant evidence which should be acceptable in the court [8]. The investigators need to be aware of the Islamic law that is followed in Saudi Arabia (Al Sharia) to be able to deal with and produce relevant digital evidence, because when a crime in Muslim society occurs, it is essential that that the evidence meets the requirement of Sharia law, which is based on the Qur'an and which states "Bring forth your proofs, if you are truthful" [1], [10].

The investigation process in Saudi Arabia is broken down into four phases. The first phase is that of seizing the suspect equipment with the appropriate lawful power to ensure that the evidence is secure and accessible. The next phase is that of the inspection of the evidence, which will attempt to prove the relationship between the suspect and the case. The third phase is where the experienced analyst seeks to connect the suspect with the case. In Islam, it is allowable to have an expert witness as pointed out in the Qur'an, "So ask of those who know the Scripture if you know not" (The noble Qur'an 16:43). The fourth phase is where answers to questions regarding what type of crime was committed, the type of evidence that has to be gathered, how it was gathered, what happened, when and by whom [3], are produced.

This research reviewed sixteen of the existing digital forensics investigation frameworks and the processes that they included. In the following section is a review of each of these frameworks.

In 1984, the original computer forensics investigation process model was proposed by Mark Pollitt, and comprised four phases: acquisition, identification, evaluation, and admission, which aimed to guarantee the admissibility of evidence in the court [16], [19], [20], [24].

Some 17 years later, Lee et al. in 2001, suggested a new model to deal with the investigation process and crime scene investigations. The steps of this model are recognition, identification, individualisation and reconstruction [21], [18], [9]. Also in 2001, the DFRWS model was proposed to be a basis to define a comprehensive model, but it was not designed to be a full model [5], [7], [24].

The abstract digital forensic model, which was proposed in 2002 by Reith, Carr and Gunsch, provides a model that can be applied to specific incidents. This model comprised nine phases: identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence [24], [2], [9], [4], [14].

Carrier and Spafford proposed the Integrated Digital Investigation Process (IDIP) Model with five phases: readiness, deployment, physical crime scene investigation, digital crime scene investigation, and review, aimed at the reconstruction of the events leading up to the incident and confirms full review of the incident, and therefore eventually builds a mechanism for faster forensic investigations [4], [24], [2], [19], [7].

The End-to-End Digital Investigation Process was proposed in 2003 by Stephenson and comprises nine phases: collecting evidence, analysis of individual events, preliminary correlation, event normalizing, event de-confliction, and second level correlation (consider both normalised and non-normalised events), timeline analysis, construction of the chain of evidence, corroboration (consider only non-normalised events). This model provides the phases to support the investigators to collect, preserve, examine and analyses digital evidence [22], [23].

In 2004, Baryamureeba and Tushabe proposed the "enhanced digital investigation process model, which seeks to separate the digital crime scene and the physical crime scene into two phases (called trace back and dynamite) to avoid inconsistencies [4].

In 2004, Ciardhuáin proposed a model to help the investigators by providing a foundation for the development of techniques and tools. The proposed model is called 'An extended model of cybercrime investigation', which consisted of a number of phases: awareness, authorisation, planning, notification, and search and identify, collection, transport, storage, examination, hypotheses, presentation, proof/defence, and dissemination [18], [21]-[23]. Also in 2004, Beeb and Clark proposed a hierarchical, objective-based framework for the digital investigations process that was in the form of a hierarchical structure which enabled the model to be more flexible and usable. This model consists of six phases: a preparation phase, incident response phase, data collection phase, data analysis phase, presentation of findings phase and incident closure phase [24], [15].

The computer forensic field triage process model was proposed by Rogers et al., to deal with digital evidence in a short time period through three phases: identification, analysis and Interpretation. This model was not designed to be appropriate to all investigative conditions [24], [21], [14].

Kohn et al. proposed a model of a fully comprehensive framework, which included the phases: Preparation, investigation, and presentation. This model provides a legal foundation to gain an understanding of the legal requirements [24].

Freiling proposed the common process model for incident and computer forensics. The aim of this model was to improve the investigation process by combining two concepts: computer forensics and incident response. This model focused on the analysis phase, consisting of a pre-analysis, analysis and post-analysis. Moreover, it offered a method to conduct analytical incident response, computer forensics, merged with forensic analysis in the incident response framework [11], [24], [21].

A Digital Forensic Model based on the Malaysian Investigation Process was proposed by Perumal, which comprised seven phases: planning, identification, reconnaissance, transport and storage, analysis, proof and defence and archive storage. This model is not suitable for use in all digital investigations, because it is not applied to all aspects of an investigation [24], [18].

Yusoff et al. proposed the Generic Computer Forensic Investigation Model after studying other investigative models. This model seeks to be a generic digital investigation model

and includes five phases: pre-process, acquisition and preservation, analysis, presentation, and post-process [24].

Hong et al. proposed a new triage model conforming to the needs of the selective search and seizure of electronic evidence. This model seeks to be helpful in meeting the demands of legal systems to protect privacy and decision making [13].

IV. A Method to Enhance the Accuracy of Digital Forensics in the Absence of Sufficient Evidence in Saudi Arabia

In this section, the researcher sought to propose a model to take advantage of all the previous models in the field of digital investigations and to take account of the responses of interviewees in conformity with Sharia law to achieve a comprehensive model in digital investigation that can be used in cases where there is an absence of sufficient information in Saudi Arabia to reduce the number of cases rejected in the courts.

After conducting a number of interviews and analysing the participants' responses, the researcher developed the framework below to enhance the accuracy of digital forensics in cases where there is insufficient information. This model emerged from analysing the data of this research (participants' interviews and literature). Interview questions encouraged the participants to explain the procedure of investigation from which the research was able to develop the investigation process including search in an investigation, inspection, expert witness and investigation presentation that works in accordance with process of investigation that is mentioned earlier.

In addition to that the answers from the respondents helped the researcher to think of a solution for dealing with cases where there was initially insufficient evidence. Therefore, the researcher developed a framework to enhance the digital investigation process in the absence of sufficient information by introducing the below framework and by adding a unique step in the investigation process, the "TraceBack Phase".

In the description phases of the proposed framework, the researcher has to reveal the relationship between each phase in an acceptable way and this framework can be of help to the investigators to understand the relationship between the phases. Therefore, the presented model is designed to achieve the required level of accuracy in an investigation and gain sufficient evidence to enable it to be admissible in court. The phases implemented in the proposed model are as follows:

A **preparation** phase is to prepare the investigation environment and includes the selection of tools and techniques and obtaining search warrants, authorization and management support. Next is the **identification** phase, which will help the investigator to identify the suspect digital equipment and the type of incident. Then **Preservation** phase is used to preserve the evidence from the crime scene without any contamination. The **Collection** phase involves the task of seizing the suspect's device(s). The **Acquisition** phase is to collect data from the suspect device(s) by using forensic tools and techniques, such as the recovery of deleted, swapped, hidden and corrupted files, and analysis to verify the relationship with the case. The **Examination** phase involves the identification, verification and validation of potential evidence which is related to the case. Next is the **Analysis** phase, which involved analysis of data, which may include the use of software tools and techniques to prove or disprove the case. The **Evaluation** phase is to determine what evidence is relevant to the case. If there is insufficient evidence found during the evaluation phase, the investigator will proceed to the **Traceback** phase which leads the investigator to further examine the suspect's devices in an attempt to obtain additional evidence or leads for further investigation, which may include the investigation of devices belonging to other suspects, with the investigation loop continuing until the case is closed. The **Presentation** phase is to present the end result (relevant data) of the process using appropriate and accepted techniques and tools. **Returning evidence** is the final phase, once the investigation process is completed, the investigator has to return the physical devices to its original owner.

V. Comparison with Existing Models

In this review, the author has arranged the reviewed digital investigation models in chronological order to identify phases common to all of the models. Afterwards, all the phases were extracted and arranged so that similar tasks were grouped together with unique identifiers according to each of the digital investigation processes, as shown in Table I. It was found that in many cases, the phases overlap each other, and in some cases are duplicated. Certainly, the multitude of digital forensics models proposed by the authors reveals the complexity of the digital forensics processes.

Table I shows a comparison of the digital investigation phases in the proposed model with those in the existing models which were discussed early.

VI. Conclusion

Based on that grouping of phases extracted from the previously defined models and frameworks, we proposed a model which is entitled "A method to enhance the accuracy of digital forensic in the absence of sufficient evidence in Saudi Arabia". This model provides investigation processes that will be accurate and comprehensive, and can be used to deal with the range of different scenarios currently being encountered in Saudi Arabia.

TABLE I
COMPARISON OF DIGITAL INVESTIGATION PHASES IN THE PROPOSED MODEL WITH THE EXISTING MODEL

Phase in the proposed model	Found in
Preservation	DFRWS Investigative Model, Abstract Digital Forensic Model, End to End Digital Investigation, Network Forensic Generic Process Model, Generic Computer Forensic Investigation Model.
Identification	Computer Forensic Investigative Process, DFRWS Investigative Model, Abstract Digital Forensic Model, Digital Forensic Model based on Malaysian Investigation Process (DFMMIP), Scientific Crime Scene Investigation Model, End to End Digital Investigation
Preparation	Abstract Digital Forensic Model, A Hierarchical, Objective-Based Framework for the Digital Investigation, Framework for a Digital Forensic Investigation, Network Forensic Generic Process Model
Collection	DFRWS Investigative Model, Abstract Digital Forensic Model, End to End Digital Investigation, Extended Model of Cybercrime Investigation, A Hierarchical, Objective-Based Framework for the Digital Investigation, Network Forensic Generic Process Model
Acquisition	Computer Forensic Investigative Process, Generic Computer Forensic Investigation Model
Examination	DFRWS Investigative Model, Abstract Digital Forensic Model, End to End Digital Investigation, Extended Model of Cybercrime Investigation, Network Forensic Generic Process Model.
Analysis	DFRWS Investigative Model, Abstract Digital Forensic Model, Common Process Model for Incident and Computer Forensics, Digital Forensic Model based on Malaysian Investigation Process (DFMMIP), End to End Digital Investigation, A Hierarchical, Objective-Based Framework for the Digital Investigation, Network Forensic Generic Process Model, Generic Computer Forensic
Evaluation	Computer Forensic Investigative Process
Traceback	None
Presentation	DFRWS Investigative Model, Abstract Digital Forensic Model, End to End Digital Investigation, Extended Model of Cybercrime Investigation, A Hierarchical, Objective-Based Framework for the Digital Investigation, Framework for a Digital Forensic Investigation, Network Forensic Generic Process Model, Generic Computer Forensic Investigation Model.
Returning evidence	Abstract Digital Forensic Model

REFERENCES

[1] Abbas, N. H. (2009). Quran 'search for a concept' tool and website. Unpublished thesis, University of Leeds. Available at http://www.comp.leeds.ac.uk/nora/html/27-64.html. Last accessed 01/07/2016.

[2] Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118-131.

[3] Al-Murjan, A., & Xynos, K. (2008, April). Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case. In Proceedings of the Conference on Digital Forensics, Security and Law (pp. 15-32).

[4] Baryamureeba, V., & Tushabe, F. (2004, August). The enhanced digital investigation process model. In *Proceedings of the Fourth Digital Forensic Research Workshop* (pp. 1-9).

[5] Bem, D., & Huebner, E. (2007). Computer forensic analysis in a virtual environment. *International journal of digital evidence*, *6*(2), 1-13.

[6] Brill AE, Pollitt M. (2006). The evolution of computer forensic best practices: an update on programs and publications. Journal of Digital Forensic Practice, 1:3–11.

[7] Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of digital evidence*, *2*(2), 1-20.

[8] Carrier, B. D. (2006). A Hypothesis-based Approach to Digital Forensic Investigations. CERIAS Tech Report 2006- 06, Purdue University, Center for Education and Research in Information Assurance and Security, West Lafayette.

[9] Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1), 1-22.

[10] Dafiri, S. (2003), In-Depth Studying of the Law on Criminal Procedure in Saudi Arabia, Dar Tibah, Riyadh.

[11] Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. *IMF*, *7*, 19-40.

[12] Glaser, B., and Strauss, A. (1967). The discovery of grounded theory. Chicago: Aldine.

[13] Hong, I., Yu, H., Lee, S., & Lee, K. (2013). A new triage model conforming to the needs of selective search and seizure of electronic evidence. *Digital Investigation*, *10*(2), 175-192.

[14] Köhn, M., Olivier, M. S., & Eloff, J. H. (2006, July). Framework for a Digital Forensic Investigation. In *ISSA* (pp. 1-7).

[15] Nicole Lang Beebe and Jan Guynes Clark. (2004). *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process.* Available: http://www.dfrws.org/2004/day1/Beebe_Obj_Framework_for_DI.pdf. Last accessed 08 Jun 2012.

[16] M. G. Noblett, M. M. Pollitt & L. A. Presley, (2000) "Recovering and Examining Computer Forensic Evidence", Forensic Science Communications, Vol. 2, No. 4.

[17] Myers, M. D., & Avison, D. (Eds.). (2002). Qualitative research in information systems: a reader. Sage.

[18] Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*, *9*(8), 38-44.

[19] Pollitt, M. M. (2007, April). An ad hoc review of digital forensic models. In*Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on* (pp. 43-54). IEEE.

[20] Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, *1*(2), 19-38.

[21] Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, *8*(10), 163-169.

[22] Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, *8*(2), 42-54.

[23] Stephenson, P. (2003). Modeling of post-incident root cause analysis. *International Journal of Digital Evidence*, *2*(2), 1-16.

[24] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology*, *3*(3), 17-31.

Fahad Alanazi is a PhD student in De Montfort University. Faculty of cyber security center. He received his B.Sc in computer science from Tabouk University in Saudi Arabia and also received MSc in Computer Security from De Montfort University. His main research interests is Computer Forensics.

Prof. Andy Jones. After a 25 year career in the British Army he became a manager and a researcher and analyst in the area of Information Warfare and computer crime at a defence research establishment. In 2002, he left the defence environment to take up a post as a principal lecturer at the University of Glamorgan (now the University of South Wales) in the subjects of Network Security and Computer Crime and as a researcher on the Threats to Information Systems and Computer Forensics. He developed and managed a well equipped Computer Forensics Laboratory and took the lead on a large number of computer investigations and data recovery tasks. He then joined the Security Research Centre at BT where he became a Chief Researcher and the head of information security research. In 2009 he moved to a post as the Programme Chair for the MSc. in Information Security at Khalifa University of Science, Technology and Research in Abu Dhabi in the UAE. He moved back to the UK in 2013 where he wrote a book on Information Operations. He

holds posts as visiting professor at Edith Cowan University in Perth, the University of South Australia in Adelaide, Australia, De Montfort University, Derby University and the University of South Wales. He holds a Ph.D. in the area of threats to information systems. He has written seven books on topics including Information Warfare, Risk management and Digital Forensics and Cyber Crime has also had more than 100 papers on the same subjects published. He is currently the director of the Cyber Security Centre at the University of Hertfordshire.