UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

# A Generic Digital Forensic Business Model: Malaysia as Case Study

Nurul Haswani Saiman and Mazura Mat Din
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
Email: nhaswanis@gmail.com, mazura@utm.my

Submitted: 12/01/2018. Revised edition: 26/03/2018. Accepted: 8/05/2018. Published online: 21/05/2018

***Abstract*— Rapid development of cyberspace has created a healthy competition in the creation of computer systems and other devices. The impact of these developments is that cyber threats had caused hectic in digital security area and its reliability to be the trusted system in the industry. Therefore, in order resolve the problem, many countries began developing their own procedures for investigating cyber-related cases based on their own law and regulations and it when the term of digital forensic take place. Researchers began to provide the best definition of each potential element that said as can be a structure in the digital forensic. On other part, the preparations of designing the investigation procedures were based on various designs. In this research, modified investigative procedures are centered on the Malaysian Chief Government Security Office as a central authority providing advisory services in the field of physical security, document security, personnel security and ICT security. The comparison between approaches had been made where it cover two approaches namely framework and business model. Based on the survey that been made within the organization, selection of design and framework for digital forensic for this organization is based on the business model in general and the Digital Forensic Business Model in particular and it will link together with the general elements and components of digital forensic.**

**Keywords — Digital Forensic, Digital Forensic Business Model, Investigation, Digital Crime, Digital Evidence**

## I. INTRODUCTION

In the age of information technology, computers are used everywhere. Cyber-attack can knock at anybody computer or device at any time or places. The attackers are constantly evolved using emerging techniques and technology in order to enter the industries. Criminals use computers to attack critical infrastructures such as the telecommunications and power distribution networks, transportation systems, and essential public utility services [65].

In Malaysia, the government under the Ministry of Science, Technology and Innovation has set up an agency under its control to deal with digital forensic matters that known as Cyber Security Malaysia (CSM). CSM is born to be a face of digital forensic enforcement in order to prevent and handle the crime. Besides, there are various enforcements that also cope with digital forensic and one of it is Malaysian Chief Government Security Office (MCGSO) that placed under the Prime Minister Department.

In an investigation, Standard Operating Procedure (SOP) is very important in order to make the process been derived smoothly. Based on Oxford Dictionary, SOP is known as standard and certified procedures that must be followed by each member in an organization or group each time the procedures been implemented. As in Malaysian government service, SOP had been said as a must in every process of services.

Digital Forensic is complicated and will evolve from time to time [8]. Preparation against this war had become important to every organization in order to protect their information. As for MCGSO, even though the case does not end up in court the case will not be admissible to the court. MCGSO must at least investigate it using a correct procedure. Digital forensic is a tiring job and thus cyber expert needs some methodologies that will guide or assist in the investigation of digital forensic.

In order to step past over the criminal, organization must aware and implement the best protective security in every step of finding, discussing, documenting and presenting the information. Digital forensics will always include at least all of these three (3) elements; human who conducts the activity, digital evidence as the main object, and the process as a reference for the activity to be followed [62].

Nowadays, MCGSO is using their own unstandardized digital forensic procedures that will be practiced by a digital investigator in carrying out digital investigation activities. The procedures are depending on cases. Concluded in their procedure are the elements of digital forensic as said above

The job space for MCGSO staff in digital forensic field was to provide protection security advice from physical aspects, documents, personnel, and ICT security. In other word, the cases that will be investigated were not specifically to be used in judgment. Simultaneously, it did not applicable in digital forensic framework approach as this kind of procedure had stated that their goal is to made the crimes been judged in the court of law. That is why, this study will focus on proposing the business model for MCGSO.

The contribution to this case study was a generic digital forensic business model for MCGSO so that the interaction between human, interaction between human and digital evidence, and interaction between human and the process of digital forensic will be applied accordance to their digital forensic procedures.

## II. Related Work

Based on the Oxford dictionary, the definition of forensic is to relate or to apply scientific practice in order to investigate cases that will be in judgment by law. Governments worldwide know that not every forensic case will end up in courts of law as for example internal investigations and disciplinary hearings [30]. Thus, [30] ascertaining that forensic will be referred as when a forensic investigation been started, the investigation it will be organized using a scientific method or practice which will be supported by law.

Some authors had defined digital forensics as the process procure and proven technical procedures and tools according to the after-the-fact digital information been attained from digital sources [60]. It is the specific reason of proceed the investigation orderly and keep on developing curiosity of events as an evidence [60]. The authors pull out the criminal element so that the digital forensic scope will be broadening to variety of investigation.

Digital forensic is well known with the three (3) basic components that are obtained the evidences, validated the evidences and analyzed the data [30]. Besides, [38] had additional component of digital forensic indicate of four components that are to collect, to examine and to analyze and to report.

- To collect refers to the identification, tagging, recording, and obtaining data thru the legal processes and sources whilst intend to make sure that the data is not been modified.
- To examine refers to the step of collecting data and simultaneously evaluate and draw out the potential evidence that definitely not been modified.
- To analyze refers to conclude the collected and examined data. If there is a need to specify additional data in detailed the investigator will need to ask for new permission to collect the data.
- To report refers to the reporting of the results based on analyzed result containing the description of actions used, the explanation on how the tools and procedures been selected, the determination on what the strategy of examination, the method to secured the exposure, the improvised of the security management and the endorsement of examination development and how it can be improved.

There were many approaches in designing a digital forensic procedure. In this study, the comparison of previous work will cover only two (2) approaches that were the digital forensic framework and digital forensic business model. Based on Oxford dictionary, framework is defined as a supporting or underlying structure. In other word, digital forensic framework can be elaborated as a tree of digital forensic structured based on the policy to achieve particular goals. For digital forensic, the goal is to be heard in the court of law. The framework discusses only the stage, methodology or investigation model that can be applied in implementing digital forensics activities. The framework will guide what should be done by a digital investigator in carrying out digital investigation activities. Some frameworks also give guidance to institutions what to be prepared to perform a digital forensics activity.

[40] described in contrast meaning which is he said business model is a theoretical appliances that comprised a conclusion about elements and its relation and the logic idea of the organization's core business. Business model also can be said as a description of the organization's value that will be offered to customers and at the same time it can be describe as a description of the organization's architecture and the people around them in order to create, market and deliver capital interaction whilst sustainably try to increase and tenable the organization's profit [40].

[51] defined clearly that a business model is not about a strategy but it is an appliances of testing and modifying the cause and effect relationship in the concept of strategy making. Hence, the theory of business model can be said as an integrated model that concludes all main strategy perspectives into one framework [26].

In this study, as MCGSO will act as an advisor to the crime, business model is selected for digital forensic approach. The gaps found in the previous business model are lack of components consistency and even if the components are same in some events there exist doubt about the acceptance of the components within the organization. Based on that, adoption completely is very difficult without modification. These limitations will initiate the research of Digital Forensic Business Model for Malaysian Chief Government Security Office.

## III. The Proposed Methodology

This study consists of three (3) phases. The first phase is the planning phase where all the information will be gathered which includes related study. Existing digital forensic business model will be analyzed and mapped to the proposed digital

forensic business model. The second phase is the designation and implementation of the proposed components of proposed digital forensic business model. The last phase will include the validating process for the performance of the proposed digital forensic business model.

Planning phase will conclude the study of digital forensic business model and the aim of this review is to gather enough knowledge that is related to the topic which is current from previous researchers. Due to the problem of the existent of various approaches in structuring the digital forensic procedure, this study only focused on two (2) existing study on approaches namely the digital forensic frameworks and the digital forensic business model. Both approaches have same objectives as it been designed in order to become a structure of standard operating procedure.

Data collection process started with the purpose of evaluating if the sample company qualifies for the digital forensic business model. For this reason, the requirement of the expert respondents as well as the openness for company based on organization's core business and event strategy analysis was investigated through the expert reviews and data search within or outside of the organization. The result will show positive acceptance and interest which led to the initiation of the practical study part.

As a next step, a new digital forensic business model for MCGSO will be drawn up with help of the collected data and the suggested data where for this purpose, internal data and secondary data will be gathered and analyzed related to the suggested steps within the business model. One type of source for the creation of the new business model was reviewing the company culture and history, a judgment on digital forensic fields and technologies as well as the past cases. Other type was searching the data over the related scenario and research outside the organization such as past research and incident.

The digital forensic business model that been designed will not be considered suitable or appropriate for MCGSO. Validation and assessment to the proposed business model is used to ensure that the business model components are appropriate or not in order to be applied over the organization's need. As mention before, the components will be validated by an expert in the field of digital forensic using the qualitative and quantitative interviews and expert reviews.

## IV. Design And Implementation

In commencing to this study, a set of expert reviews had been created and been distributed to expert respondents in MCGSO. These expert respondents were from different type of position and department. The relevance of their selection was based on their involvement of the investigation in digital security breaches. , the experts that act as respondents are coming from MCGSO HQ; ICTRR department and Inspectorate department, MCGSO Kedah, MCGSO Perak and Hospital Sultanah Aminah. Total of the experts is eight (8) people consist of two (2) women and six (6) men. Two (2) from the experts are the Security Assistant where their job scope is assisting the investigation process made by their officer. Meanwhile, three (3) from them are the Deputy Director and two (2) from them are the Assistant Director. The last expert is coming from Hospital Sultanah Aminah as a Head of Security Division.

The purpose of the expert reviews was to find out about the significance of proposing the digital forensic business model in MCGSO and at the same time to gain knowledge about current state of how they conducting their digital forensic investigation. The expert reviews been divided into three (3) section namely Section A, Section B and Section C and it will be shown below.

Section A is for identification of the experts. From Section A, the conclusion was all expert respondents had work in the security field in between 1 to 10 years. Two (2) of them are woman whilst the other is men and all of them are full time staff. In term of expertise; six (6) of them are an officer in their department or states whilst two (2) of them were the assistant security officer in ICTRR.

Section B and C that contain three (3) questions (Q) in each Section and the answer will give the gist of this phase. Section B focused on existing Standard Operating Procedure in MCGSO. The questions are as below:

- Q7: "Do you believe that Standard Operating Procedure (SOP) is necessary in every operation in your organization? Please give reasons for your response."
- Q8: "Do you deal with matters related to the investigation of the security breach through computer or other devices? How many times in a year that situation occurs?"
- Q9: "Do you have a SOP for the investigation? Assuming that the respondents know about the Digital Forensic Framework, did the SOP of the investigation follow the Digital Forensic Framework?"

Section C focused on the Proposed Digital Forensic Business Model and The questions are as below:

- Q10: "Assuming the respondents know about the Digital Forensic Business Model, do the Digital Forensic Framework that been used in your organization had been adjusted with a Digital Forensic Business Model?"
- Q11: "Do you believe that if the incident occurs and your organizations taking an action using the Digital Forensic Business Model, the investigation period and cost will be reduce? Please give reasons for your response."
- Q12: "Do you believe that if the incident occurs and your organizations taking an action using the Digital Forensic Business Model,the investigation period and cost will be reduce? Please give reasons for your response."

Based on their answer in Q7, all of the experts agree that standard operating procedure (SOP) is necessary in every operation in their organization. Some of them said it is because to make the job done with structured. Meanwhile, the other said the existent of SOP will make work done easily and exaggeratedly.

Q8 focused on expert's experiences. Some of them said they had gone through a situation where the security breach of information arises but the situation is not worst. Some respondent said they had not experienced it even once.

Q9 show the very importance part of this expert reviews. This question focused on their way of investigates the security breach cases. Apparently, MCGSO's officer investigate each cases that arise based on the cases structure or scenarios and it give a conclusion that MCGSO did not have standard SOP in doing their investigation of digital security breach. This fact give the big impact of this study explicitly as it showed that this organization needs an approach of digital forensic.

In Section C, there exists confusion among the respondents as expert_1, expert_2 and expert_6 did not really understand about the digital forensic business model. Other respondents clarify that the existence of digital forensic business model gives huge benefit and guidance in order to make a better investigation process.

As a conclusion, there is a need in designing and documenting an approach to digital forensic for MCGSO. As almost all the expert said that it will be an effective way to do the investigation.

In strengthening the decision, secondary data such as closed interview thru Whastapp and data from the MCGSO website also had been adapted. In other side, the existing framework and business model component for forensic business model were reviewed so that the important components will be identified. The main components of the digital forensic business model will be revised from previous study as in Table I.

The first component that called value proposition is the overall view of the product and services offered to the client and addresses how and what is the proposed solution to offer over the targeted client when problems occur.

Next component is value architecture that describes the changes that can be made if roles and capabilities in value proposition are changed. Value finance and profit is the next component and it involves the economical aspect of the business process in order to increase profit and it is essential to be associated with value proposition and value architecture.

Customer value proposition is the process or activities to make sure there are a connection between the customer and the organization. It also describes the value that is offered by the organization to the customer/client. Key resources are a component that portrays the key resources and disclose how the organization delivers the value and the operation used in the process. It usually involves the people, technology and equipment used in the process.

The next component is called key process that describes the step by step activities that are done in order to deliver the value to the client depending on some rules and matrices that are suitable. Value network represents the technical resources involving the suppliers, customers within and between the businesses. It also defines the flows of the services and the information used so that it does not exit the boundary.

TABLE I. REVISED COMPONENTS FOR PROPOSED DIGITAL FORENSIC BUSINESS MODEL

| Authors / Components | Al-Debei et al, 2010 | Shafer et al, 2005 | Johnson et al, 2008 | Osterwalder et al, 2010 | Fjelts, 2011 | Kaplan, 2012 | Yudi et al, 2015 |
|---|---|---|---|---|---|---|---|
| Value proposition | √ | √ | | √ | √ | | √ |
| Value architecture | √ | | | | √ | | |
| Value finance and profit | √ | √ | √ | √ | √ | √ | |
| Customer value proposition | | √ | √ | √ | | √ | √ |
| Key resources | | | √ | | | | |
| Key processes | | √ | √ | √ | | √ | √ |
| Value network | √ | √ | √ | √ | | √ | √ |
| Exploration, analysis and presentation | | | | | | | √ |

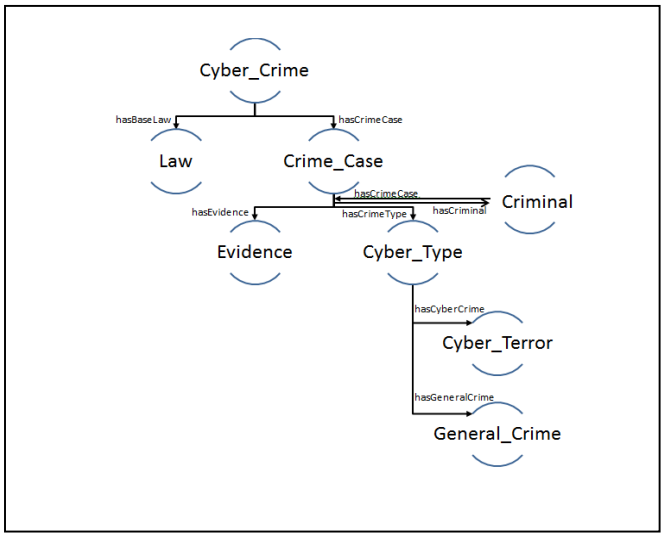


Fig.1. Concept Diagram in Digital Forensic Crime (Park *et al*., 2014)

The last component is exploration, analysis and presentation which contain the summarization of the results that are processed and analyzed. After that, the results are then will be presented to the higher ups and clients. After analyzing the existing components and based on the Concept Diagram in Digital Forensic Crime by [27] as in Figure I, Table II has been made to summarize the components according to the basic and generic business model component.

TABLE II. REVISED COMPONENTS FOR PROPOSED DIGITAL FORENSIC BUSINESS MODEL

| Components | Revised Components |
|---|---|
| Value proposition | Value Creation |
| Value architecture | |
| Value finance and profit | |
| Customer value proposition | Value Capture |
| Key resources | |
| Key processes | Value Delivery |
| Value network | Summarization |
| Exploration, analysis and presentation | |

## V. CONCLUSION

Apparently, this study had shown the accommodation of major components in digital forensics (human, digital evidence, process) using the business model. Based on the agreement of the experts from this organization, the digital forensic business model that will be designed and will be named as Generic Digital Forensic Business Model.

## REFERENCES


[1] Abdalla *et al*. (2007). Guideline Model for Digital Forensic Investigation Annual ADFSL Conference on Digital Forensics, Security and Law. 2.

[2] Ademu. (2011). Digital Forensic Acquisition and Analysis Tools and Its Importance.

[3] Agarwal *et al*. (2011). Systematic Digital Forensic Investigation Model.

[4] Al-Debei *et al*. (2008). Defining the Business Model in the New World of Digital Business.

[5] Al-Debei *et al*. (2010). Developing a Unified Framework of the Business Model Concept.

[6] Al-Hadadi and AlShidhani. (2013). Smartphone Forensics Analysis: A Case Study. International Journal of Computer and Electrical Engineering, 5(6).

[7] Al Hogail. (2015). Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study.

[8] Aswami *et al*. (2008). Digital Forensics in Malaysia.

[9] Barske. (2010). A Digital Forensic Readiness Framework for South African SME's.

[10] Beebe. (2009). Digital Forensic Research: the Good, the Bad, and the Unaddressed.

[11] Carrier *et al*. (2003). Getting Physical with the Digital Investigation Process.

[12] Carrier. (2013). Open Source Digital Forensics Tools.

[13] Chawki. (2004). The Digital Evidence in the Information Era.

[14] Chesbrough *et al*. (2002). The Role of the Business Model in Capturing Value from Innovation.

[15] Chesbrough. (2010). Business Models Innovation: Opportunities and Barriers.

[16] Chhabra *et al*. (2015). Distributed Network Forensics Framework: A Systematic Review.

[17] Cohen. (2013). Digital Forensic Evidence Examination.

[18] Dezfoli *et al*. (2013). Digital Forensic Trends and Future.

[19] Elyas *et al*. (2014). Forensic Readiness: Is Your Organisation Ready?

[20] Elyas *et al*. (2015). Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework.

[21] Fielts. (2011). Business Service Management Whitepaper.

[22] Gilad. (2011). Business Strategy Series. Strategy without Intelligence, Intelligence without Strategy, 4-11.

[23] Gita. (2014). Digital Evidence in Malaysia.

[24] Grobler *et al*. (2007). Digital Forensic Readiness as a Component of Information Security Best Practice.

[25] Grobler *et al*. (2010). A Framework to Guide the Implementation of Proactive Digital Forensics in Organizations.

[26] Headman *et al*. (2003). The Business Model Concept: Theoretical Underpinnings and Empirical Illustrations.

[27] Park *et al*. (2009). Cyber Forensics Ontology for Cyber Criminal.

[28] Investigation Huang. (2015). A Framework of Network Forensics and its Application of Locating Suspect in Wireless Crime Scene Investigation.

[29] Johnson *et al*. (2008). Reinventing Your Business Model.

[30] Kaplan *et al*. (2012). The Business Model Innovation Factory: How to Stay Relevant When the World is Changing.

[31] Kohn *et al*. (2006). Framework for a Digital Forensic Investigation.

[32] Kohn *et al*. (2013). Integrated Digital Forensic Process Model.

[33] Krueger *et al*. (2001). Designing and Conducting Focus Group Interviews.

[34] Kruse *et al*. (2002) Computer Forensics: Incident Response Essentials.

[35] Mager *et al*. (2007). Standard Operating Procedure for the Collection of Fresh Frozen Tissus Samples.

[36] Magretta *et al*. (2002). Why Business Models Matter.

[37] Mansfield. (2004). Strategy and Business Models.

[38] Martini *et al*. (2012). An Itegrated Conceptual Digital Forensic Framework for Cloud Computing.

[39] NIST. (2006). Guide to Integrating Forensic Techniques into Incident Response.

[40] Oliveira *et al*. (2011). Business Model Generation: A Handbook for Visionaries, Game Changers and Challengers.

[41] Osterwalder. (2004). The Business Model Ontology: A Proposition in a Design Science Approach.

[42] Paulo *et al*. (2013). Computer Forensic Laboratory: Aims, Functionalities, Hardware and Software.

[43] Perumal. (2009). Digital Forensic Model Based on Malaysian Investigation Process

[44] Perumal *et al*. (2011). New Improvement In Digital Forensic Standard Operating Procedure (SOP).

[45] Perumal. (2012). Digital Forensic Investigation Model Based on Malaysian Standards with Live Forensic Investigation Tool.

[46] Pollitt. (2001). A History of Digital Forensics.

[47] Rasmussen. (2007). Business Models and the Theory of the Firm.

[48] Reyes *et al*. (2007). Developing an Enterprise Digital Investigative/Electronic Discovery Capability.

[49] Rowlingson. (2004). A Ten Step Process for Forensic Readiness.

[50] Scott. (2007). Issues of Privacy and Information Securiy.

[51] Shafer *et al*. (2005). The Power of Business Models.

[52] Sindhu *et al*. (2012). Digital Forensics and Cyber Crime datamining.

[53] Sumaiyah *et al*. (2011). The Relationship between Business Model and Performance of Manufacturing Small and Medium Enterprises in Malaysia.

[54] SWGDE. (2000). Proposed Standards for the Exchange of Digital Evidence.

[55] Taylor *et al*. (2007). Specifying Digital Forensics: A Forensic Policy Approach.

[56] Teece. (2010). Business Models, Business Strategy and Innovation.

[57] Teresa. (2010). A Conceptual Framework to Manage and Audit Information Systems Security.

[58] The Government of Japan. Agreement between the Government of Japan and the Government of Australia on the Security Information.

[59] von Solms *et al*. (2006). The Relationship between Digital Forensics, Corporate Governance, Information Technology Governance and Information Security Governance in Digital Crime and Forensic Science in Cyberspace.

[60] Willassen. (2005). Forensics and the GSM Mobile Telephone System.

[61] Yasinsac *et al*. (2001). Policies to Enhance Computer and Network Forensics.

[62] Yudi *et al*. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia.

[63] Yunus *et al*. (2011). Common Phases of Computer Forensics Investigation Models.

[64] Yutaka. (2004). Basic Structure of Government Auditing by a Supreme Audit Institution.

[65] Zahri *et al*. (2014). Adoption of ISMS for Protecting SCADA Systems against Cyber Terrorism Threats

[66] Zott *et al*. (2010). The Business Model: Theoretical Roots, recent Developments and Future Research.