Journal of Theoretical and Applied Information Technology
31st January 2018. Vol.96. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTIVIEW BUSINESS MODEL FOR DESCRIBING A MECHANISM OF HANDLING PHYSICAL AND DIGITAL EVIDENCE IN DIGITAL FORENSICS

[1]YUDI PRAYUDI, [2]AHMAD ASHARI, [3]TRI KUNTORO PRIYAMBODO

[1,2,3] Department of Computer Science and Electronics, Gadjah Mada University, Indonesia
[1]Department of Informatics, Universitas Islam Indonesia, Yogyakarta Indonesia
E-mail: [1]prayudi@uii.ac.id, [2]ashari@ugm.ac.id, [3]mastri@ugm.ac.id

ABSTRACT

Digital evidence should be handled by the same mechanism with the physical evidence. Both types of such evidence should be complementary to support the investigation and data required in digital forensics activities. An appropriate business model is required to be able to support this mechanism. The existing business models, not yet able to explain the relationship between the three principal components in digital forensics: People who run activities, Digital Evidence as the primary object and Process which serves as a guide in conducting digital forensics activities. This study proposes a business model known as 3IR (Initiative-Investigative-Interactive-Report) as a multiview business model that can describe the relationship between the People - Digital Evidence - Process that must be understood in the activity of digital forensics and digital evidence handling. The proposed multiview business model has been able to provide an overview of how the mechanism is supposed to handle digital evidence to match the handling of physical evidence. The 3IR multiview business model is supposed to be used as a reference to comprehensively describing how to handle digital evidence in any digital forensics activities.

Keywords: *Business Model, Digital Forensics, Physical Evidence, Digital Evidence*

1. INTRODUCTION

The increasing cases of cybercrime as reported by [1] [2] had a direct impact on the growth of electronic evidence handled by the digital forensics laboratory [3]. This growth was affected by the increasing volume of digital evidence which processed by the investigators as well as the increasing complexity of the management and documentation of digital evidence [4]. This condition is in line with the statement of [5] which states that the number of criminal cases has resulted in the emergence of new problems regarding control and maintenance of evidence. Common obstacles encountered in the handling of evidence is the absence of procedures and protocols of how to transfer the evidence between the divisions and the lack of integrated information systems that support the management of evidence. Although this opinion focus is on the physical evidence, the statement of [5] is also applied regarding the handling of digital evidence.

In this case, there are two almost identical terms, electronic evidence and digital evidence. Electronic evidence is physical evidence. Electronic evidence, are physically and recognizable (computers, mobile phones, cameras, CDs, USB, hard drives, etc.), while digital evidence is evidence extracted or recovered from electronic evidence (files, email, sms, image, video, logs, text). The simple definitions of digital evidence are any information of probability value that is either stored or transmitted in digital form [6], or information stored or transmitted in binary form that may be relied upon in court [7].

However, in the presence of two almost identical terms of electronics and digital, hence a more relevant definition of digital evidence is as a digital form of the output of the acquisition process and disk imaging of electronic evidence. Thus, a hard drive, mobile phone, USB is an electronic evidence, then the disk imaging result of the hard drive is a form of digital evidence. Also, regarding live forensics then digital evidence shall be any tangible file with any extension as an output of the live acquisition. While for multimedia forensics, digital evidence is any multimedia file (text, image, video, audio) that require further analysis process.

Physical and digital evidence has different characteristics, but in principle, several important aspects regarding handling evidence must have the

Journal of Theoretical and Applied Information Technology
31st January 2018. Vol.96. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

same procedures or protocols. The evidence, either physical or digital will complement each other in the process of investigation [8]. However, according to [9], [10], the handling mechanism of digital evidence is still not fully complied with the procedures and provisions of applicable law. For example, those relating to the storage and documentation of digital evidence or chain of custody. In this case, based on the experience of interacting with digital forensic practitioners who perform the handling of various cases of cybercrime, it turns out there are gaps in the handling of digital evidence as compared with the physical evidence. Based on some facts from the real conditions of handling digital evidence, the transfer of digital evidence from one investigator to another investigator is done without clear procedures and controls. This fact should not happen because it would be difficult to control the integrity of digital evidence that is being analyzed.

The key to the handling of physical evidence is the existence of the evidence storage procedure as well as the documentation into a physical form with the supervision of the officer who controls the evidence room and the documentation of the physical evidence. This is not found in the handling mechanism of digital evidence. The handling of digital evidence that has been practiced among practitioners and law enforcement is not based on the basic concept for the storage of digital evidence. The storage mechanism is oriented to the storage of physical evidence.

Digital evidence has some characteristics that are more complex and are highly susceptible to change [11], this is the reason why there are difficulties in handling digital evidence. The problem has then led to gaps digital evidence handling that is not in line with the mechanism of physical evidence. The occurrence of such gaps identified in the absence of the integrated concept to support mechanisms of digital evidence handling.

The integrated concept includes at least two aspects; the first is the concept of storage and chain of custody of digital evidence (documentation) and the second is the business model that supports the implementation of the first concept. In this case, a solution to overcome the first aspect, that is a solution for a storage of digital evidence and its chain of custody, has been proposed by [10] through the concept of Digital Evidence Cabinets (DEC).

Furthermore, to implement the DEC as the concept of storage and chain of custody of digital evidence it needs the support of a business model that provides a good illustration of how the mechanism of centralized storage and its documentation can be implemented and how the interaction between the officer with digital evidence should be done.

The needs of the business model are driven by the diversity of interpretation in the activity of digital forensics and digital evidence handling by

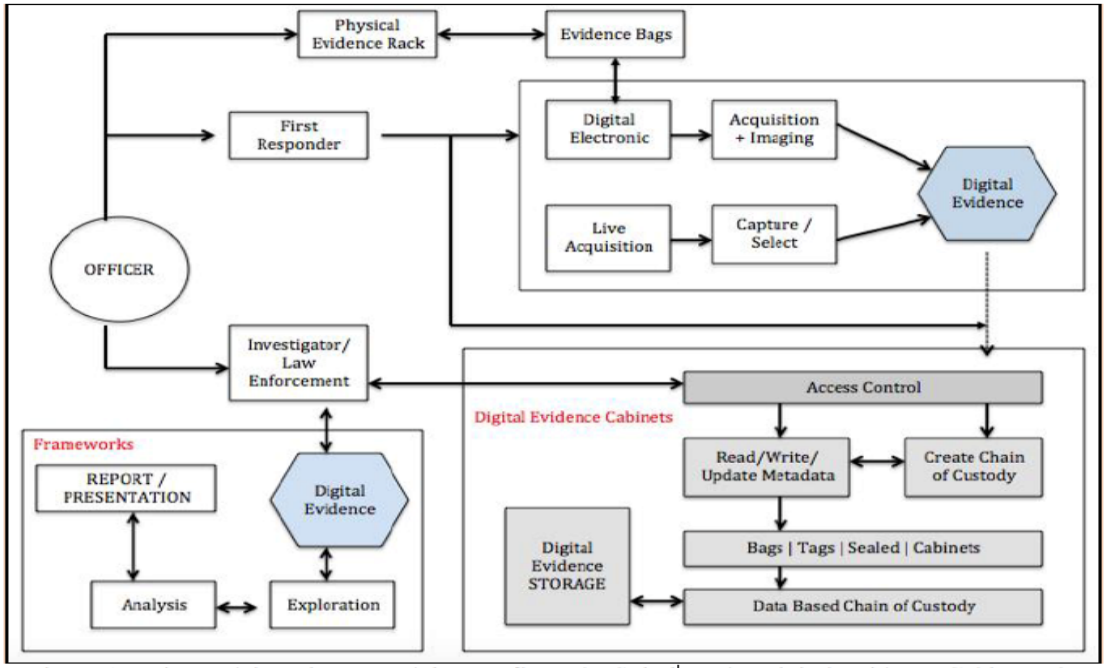

Figure 1 Early Model Business Model To Reflect The Solution The Digital Evidence Cabinets [9]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the investigators or practitioners. There should be a proposed concept that is expected to be widely accepted among the investigator or practitioners. All parties should have the same point of view in the understanding of digital evidence handling. The availability of a business model is becoming the initial strategic solution. The business model will provide a comprehensive picture of how the vast scope of digital forensics. The activity of digital forensics and digital evidence handling is not enough to be explained concerning to the framework/ methodology/ stages/ phase/ steps, but should also refer to the general picture of how the interactions between all the objects involved in the activity of digital forensics.

There are many frameworks to perform digital forensics activities. The number and the framework development process cannot be separated from the fact that is happening today; digital forensics activities are mostly dominated by practitioners. In this case [12] argues that the digital forensics studies tend to be investigator based, personal experience and expertise as well as the specific device or ad hoc basis. This is line with the opinion of [13] that the development of digital forensic science is a practitioner-driven. Many frameworks as researched by [14] and [15] have been indirectly affected by the existence of that fact.

Digital Forensics activities will always involve at least three (3) main components, namely: (1) People who perform the activity, (2) Electronic Evidence and Digital Evidence as for the primary object, and (3) Process as a reference to the steps that must be followed. The terminology of frameworks, methodologies or digital forensics phase tends to only discuss the third component. Some of the existing frameworks do not provide an illustration of how the interaction between people and the interaction between people with digital evidence as well as the interactions between people with the process itself. The framework approach that has been developed by researchers, also do not give an idea of how the process of transfer of digital evidence as well as the interaction of each person involved in the digital evidence handling. The approach of phase terminology as proposed by several researchers such as [14][15] [16] [17] [18] was not under requirements to portray the interaction between people, digital evidence and processes applied in digital forensics activities.

Prayudi in [9] has tried to propose a simple business model for digital forensics activities. This simple description is needed to provide as early illustrations of how the mechanism of Digital Evidence Cabinets (DEC) as a solution for digital evidence handling and its chain of custody. A simple overview of the business model in Figure 1 provides an illustration of the role of Digital Evidence Cabinets in the context of digital forensics. However, the business model has not contained a detailed explanation of how the interaction between the People-Digital Evidence-Process in the various phases of the investigation. This weakness then needs to be clarified in future studies

Furthermore, the framework and investigation models which have been discussed by the researchers did not give an illustration of how the transfer of digital evidence during the investigation. According to [19], the digital evidence will always be involved in every phase of the investigation, so there must be a clear clarification of how the role of digital evidence in any such phase. Proposed business model in this paper is expected to provide a digital evidence workflow and the role in every phase of the investigation. The business model is supposed to be used as a reference to comprehensively understand how to handle digital evidence in any digital forensics activities.

Then, this paper will discuss various studies about the business model issue, the methodology how the development process of business model, the proposed and the analysis of the proposed business model.

2. RELATED WORKS

The implementation of digital forensics by law enforcement agencies must be supported by a transparent procedure and mechanism of physical and digital evidence handling. In this case, a business model for digital forensics, especially to describe the storage of digital evidence and its chain of custody is a necessity for any law enforcement agency. The business models, should be able to explain how the three elements: the officers involved (first responder, officer in the storage of evidence, the investigator), the digital evidence (the handling of electronics evidence, the process of obtaining digital evidence, storage and access to evidence) and the process (the phase of exploration, analysis, reports, and presentations) can be connected to each other in an integrated workflow. Unfortunately, there has been no comprehensive study concerning the issue of the business model regarding digital forensics, in particular on the storage of digital evidence and its chain of custody. On the other hand, according to [20], the concept, assessment, and digital forensics tools were partial to conduct exploration of digital evidence does not yet support the investigative

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

process as a whole so the business model approach will be one of the solutions to that problem.

According to Kirchmer (2009) in [5], a business model consists of a set of functions that provide sequences input or output to the internal or external customer. In another view, according to [21], the business model is "an abstract representation of an organization." Meanwhile, according to[22], the term business model is used to represent a significant aspect of business. The business model can be a conceptual, textual or graphical form that provides the connectivity, collaboration or planning of all the components involved in the core business of the institution. In the context of digital forensics, a business model will provide an overview position and interrelation of all elements that perform the activity at each phase of digital forensics activities. The differences in business models will lead to differences in digital forensics activities, including the digital evidence handling and its chain of custody.

In general, the approach had been undertaken by some digital forensics researchers to describe the business model is to use the investigative phase. This approach is a step by step guide to perform digital forensic activities. In this case, the term used to describe such a guide is a framework. According to [23] framework regarding of digital forensics is "structure to support a successful forensic investigation." Based on the literature, there are many different types of frameworks, methodologies or steps that must be followed in conducting digital forensic activities. In addition to a framework as a guide, there is also another perspective: the work environment or business models. This is what was stated by [24] when discussing the various dimensions of digital forensics in an investigation activity.

Although there are many variations of digital forensics frameworks, essentially there is no difference in principle because in every framework proposed by the researchers showed only a difference of names and details of digital forensics activities [24][25][26]. Among the framework ever developed, one of them is the IDFIF (Integrated Digital Forensics Investigation Frameworks) which has developed by [18] [19].

Digital forensics activity will involve some parties. According to [29] and [30], digital forensics activities will involve first responder, digital investigator, court officer, expert witness, attorney/prosecutor, judge, police officer, the victim, suspect and passerby, prosecutor, lawyer/defense. Supposedly there is also the flow of the interaction between the parties as well as how they interact with digital evidence in the overall investigation. Each party has a different role in each phase of the digital forensics activity; then it is necessary for the mapping to see how the role of each of these parties in all phases of digital forensics. This mapping will generate a complex business models that demonstrate the interaction of the various parties involved in the digital forensics process and digital evidence handling.

Only a few papers focused on business models for digital forensics, one of them is discussed by [31] using the approach 2IR Methodology (Initiation, Investigative and Reporting) to describe the environment of digital forensics which includes several aspects, namely: education, technical, legal and ethical. This model can be used as a starting point for developing a business model for digital forensics and its chain of custody. Another model proposed by [29] namely life cycle of digital evidence that was built using Petri Nets approach. This model can also be used as a reference for developing the business models of digital forensics. The description of the business model that leads to the issue of chain of custody has been delivered by [4] through e-CoC models which later extended as a CF-CoC. This model was built to meet the needs of documentation and publication of information provenance metadata in the chain of custody [32].

Although not directly use the term of business model, but there are some digital forensics model is discussed in detail by [33] leading to the meaning of the business model as well as CFFTPM model from [34], Common Process Model from Freiling & Schwittay, Digital Forensic Model Based on Malaysian Investigation Process from [35] Digital Forensic Model from [25]. According to [33], from a variety of paper which he has compiled, came to the conclusion that all the models that have been developed so far are specific aspects of the digital forensic field only, there is no digital forensic investigation model that was developed to facilitate investigators that working in various areas of digital investigation.

When referring to one of the definitions of the chain of custody, “a procedure to perform chronologically documentation of evidence” [30], then some frameworks that have been developed for example GCFM [14] and SRDFIM [15] was also not able to give an overview of the digital evidence handling and its chain of custody. The storage mechanism and documentation of digital evidence have not been seen in both frameworks examples. The focus of that framework is as other frameworks in general, i.e., at the phase of digital forensics activities in general. A description of how

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the transfer of digital evidence and how the interaction between people involved in the process of handling digital evidence and the investigation does not appear in these frameworks.

Based on the explanation of the meaning of framework from [21] and [22], then the appropriate solution to describe the mechanism of interaction between People - Digital Evidence - Process is through a business model approach which would explain the digital evidence handling workflow and its chain of custody. In this case, the research conducted by [24] [29] and also from [4] [32] [31] can be used as a starting point to build a relevant business model.

3. LIMITATION OF THE PROPOSED MULTIPLE BUSINESS MODEL

There are many phases in the law enforcement process, one of which is the investigation phase. Digital forensics activities are one of the phases of an investigative process that will support the investigation process through the delivery of facts and data from electronic evidence and digital evidence obtained during the analysis process. The results of the analysis will then be submitted either in the form of reports or presentation to stakeholders who request digital evidence analysis services.

Therefore, the business model developed will only illustrate how the process of handling digital evidence should be done, from the initial process of obtaining electronic and digital evidence to finally submit a report or presentation of the findings requested by the investigator. The process after the digital forensics report, although still in the law enforcement phase but not included in the study of this business model.

4. RESEARCH METHODOLOGY

This study focused on the development of a relevant business model to support the concept of handling physical and digital evidence. An early model which has been generated as in Figure 1, needs to be re-design by considering other models like the model proposed by [4] [29] [31].

One of the references to build a business model is a methodology that has been done by [4] in providing solutions to the e-CoC. In this case, to get a business model, the first step taken by [4] is to choose a framework as a reference solution, which is chosen DFPM (Digital Forensic Process Models) from Kruse as a reference of the e-CoC. This approach can be used as a reference methodology in building a business model in similar studies.

However, the 2IR model from [31] was used as a reference for the development of business models in this study. The 2IR model indirectly gives an overview of how the evidence handling as well as some of the basic requirements of an officer who will handle the evidence. But the 2IR model only provides guidance on how a general overview of digital forensics activities. The 2IR models do not describe how the mechanism of interaction between the officer and the evidence. Evidence as the primary object of a digital forensics activity is not explicitly mentioned, as well as how the documentation of the evidence. For that reason, it needed the additional phase, which will explain how the interactions that occur between officer with evidence.

Table 1: Phase Description of 3IR Model.

Phase	Activity	Output
Initiative	Scene investigation of the cases involving electronic/digital evidence	Digital Evidence
Interactive	Interactions between People with electronic evidence, digital evidence, computer system	Access Control to the electronic evidence, digital evidence, and chain of custody.
Investigative	Exploration and analysis process to obtain digital evidence findings	Digital Evidence findings that relevant to the purposes of the case being analyzed
Report	Documentation digitally or physically to: digital chain of custody, findings of digital evidence, general documentation of cases being analyzed.	Final report and activities to create/ update/ Write of information both physically/ digitally or in other written documents.

The other approaches may also refer to the use of four phases as proposed by Freiling & Schwittay (2007) in [33] namely: Pre-Incident Preparation, Pre-Analysis Phase, Phase Analysis and Post-Analysis Phase. There is also another proposed phase, the use of five phase by [36], namely Preparation, Collection and Preservation, Examination and Analysis, Presentation and Reporting and disseminating the Case. However,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the use of three phases from [4], [29], [31] [31] namely: Initiative, Investigative and Report (2IR) is more simple and covers all the phases described by other researchers. Also, the meaning contained in Initiative, Investigative and Report is more flexible and to be improved to produce a business model that is expected.

Referring to the 2IR model from [31][4] [27] [29], then to clarify the relationship of each component of the business model needs additional information that describes the interactions between People - Digital Evidence - Process. Therefore, in addition to phase Initiative, Investigative and Report, another phase that needs to be added is the Interactive phase. This interactive phase shows part of digital forensics activity where there is direct interaction between people and activities with the object of digital evidence and its role in the process being run. For that matter, the next subsequent identification of the overall phase of digital forensics given a name as 3IR (Initiative, Interactive, Investigative, and Report) model. Table 1 describes the main activities and outputs of the 3IR model developed from previous models 2IR.

Furthermore, the process of developing a business model performed with the following steps:

a. Mapping the three main components in a digital forensics activity: People, Digital Evidence and Process.
b. People and Digital Evidence be detailed into several types according to the study of literature. In this case, the components of People will be divided into four different types, namely:
   - P1: Officer in Digital Evidence Room (Computer Area), they are responsible for handling the management and control of digital evidence. Digital evidence will be stored in the system with access control rights acquired through the authorization made by this officer.
   - P2: Officer in Physical Evidence Room (Physical Area), they are responsible for handling the management and control of electronic evidence. Electronic evidence stored in the evidence room with the supervision of authorized personnel
   - P3: Investigator/ Prosecutor/ Judge/ Lawyer/ Private Investigator, Law Enforcement/ Investigator: those who perform a series of processes/ digital investigation/ analysis.
   - P4: First Responder Team, they are directly responsible for the handling of electronic evidence and the process to obtain digital evidence.

   The Digital Evidence can be divided into four different types, namely:
   - D1: Digital Evidence Cabinets is an integrated system that is prepared to handle digital evidence storage mechanism as well as the chain of custody.
   - D2: Digital Evidence File, the real evidence that became the primary object of the investigation.
   - D3: Digital Evidence Finding, the finding of digital evidence as output of exploration and analysis activities.
   - D4: Electronic Evidence, physical forms of potential evidence obtained from the activity of crime scene investigation.

   The third component is Process, this component to accommodate all the steps or phase are advised to apply the forensics activities of any reference framework.

c. After an overview of business model mapped among the three components of People, Digital Evidence and Process, then the next step is to map the workflow that has been built by a group of phases. Definition of phase as in Table 1 serves as a reference for determining whether an activity included in one phase.
d. The next step is to analyze whether the business model that has been developed has met the needs of investigator or practitioners in conducting digital forensics and how business models have complied with the necessity of the application of the concept of handling physical and digital evidence.

5. THE RESULT OF PROPOSED MULTIPLE BUSINESS MODEL

Based on the evaluation, then the re-design process to obtain new business models is done using BPMN (Business Process Modeling Notation) Tools v.2. BPMN is a modeling language for developing business models, BPMN approaches have been commonly used as an option for other researchers to implement the solution business model [37]. BPMN is a standard for business process modeling that provides a graphical notation for determining business processes that occur within Business Process Diagrams (BPD). BPMN provides a way to communicate about business processes for management, business analytics, and developers, making it easy to define and analyze both general and personal business processes. There are three main categories of elements of BPMN,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

namely; Flow objects, connecting objects, swimlanes. The results of the study of a relevant business model to support the concept of handling physical and digital evidence are as in Figure 2

The result of the 3IR business model can be viewed as a Multiview Business Model. The business model is the result of a merger of two viewpoints, namely: digital forensics component (People -Digital Evidence - Process) as well as the investigation phase (Initiative-Interactive-Investigative-Report). Through the combination of these two aspects, it can be seen how the transfer of digital evidence and how the interaction of people against the digital evidence. In this business model is seen also seen who is responsible for the digital evidence. The graphics Display of the 3IR business model provides an overview of connectedness and cooperation of all the components involved in the core business of law enforcement institutions which perform digital forensics activity.

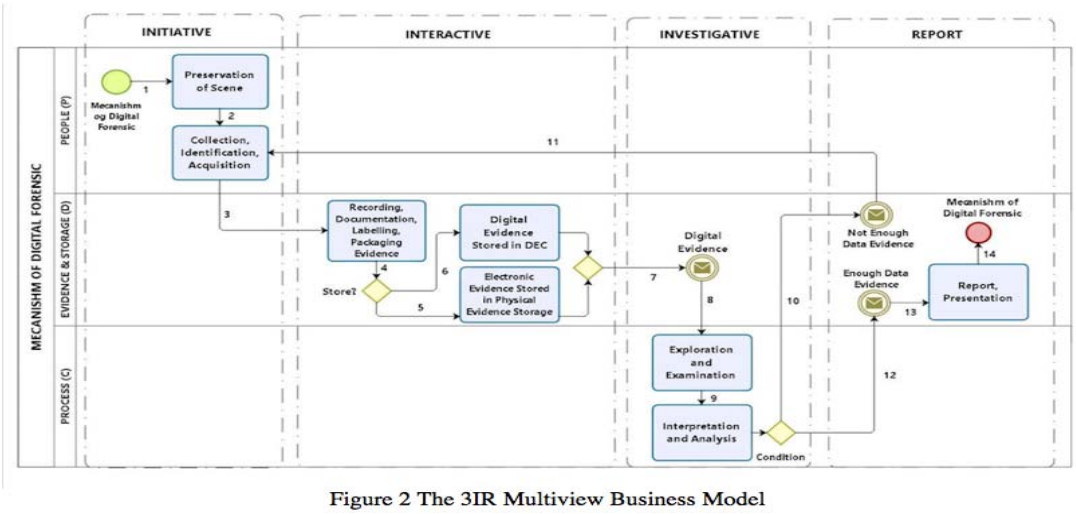

Figure 2 The 3IR Multiview Business Model

The 3IR business model can be explained as Follows:

a. The First Responder will take on an important role in the initial process of crime scene evidence through confiscation of some electronic evidence (computer, hard disk, memory, HP, USB, etc.). After making the initial identification of relevant physical information on electronic evidence, then the next step is to perform the imaging process of any electronic evidence.
b. Imaging process can be done with the help of any tools that can perform the imaging process. The output of this process is gained image files and keys hash of the file. In this imaging process, it is possible any tools generate an image file with an extension of various formats.
c. The next step is to enter file imaging has been obtained as well as basic information from the file system into the Digital Evidence Cabinets as the main storage of digital evidence. While electronic evidence physically will be deposited into the evidence room. There is an officer who will be responsible in particular to control the storage of electronic evidence and digital evidence.
d. The Digital Evidence Cabinets system would apply access control management and the documentation of every transaction of digital evidence (copy, transfer, access). On the other hand, this system will also collect some dynamic information from transaction activity carried out by someone with a digital evidence that was stored in storage.
e. The information in a specific format, for example: the name of the case, the findings on the initial information of electronic evidence, the imaging process, first responder, hash key, and the access log file and transactions will be part of the information of the digital chain of custody that is maintained by a system of Digital Evidence Cabinets (DEC).
f. Furthermore, Investigator will carry out exploration activities and analysis of digital evidence by first requesting access to the Digital Evidence Cabinets to acquire digital evidence to be analyzed. Investigators are then running a series of exploration and analysis on his computer system. The output of this activity is gained digital evidence findings that are relevant to the needs of the case being investigated.

Journal of Theoretical and Applied Information Technology
31st January 2018. Vol.96. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

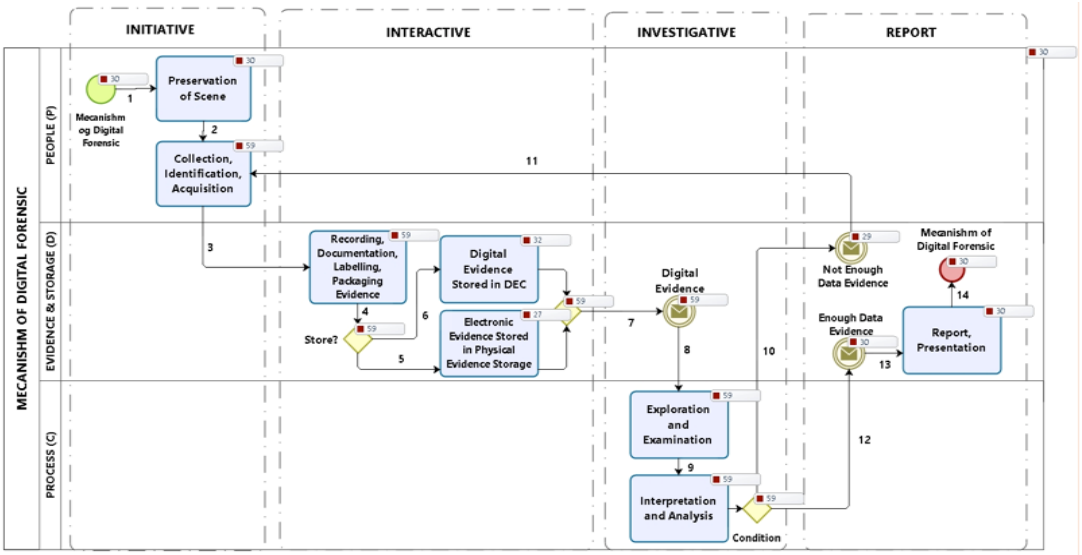

Figure 3 The Validation Model of 3IR Multiview Business Model

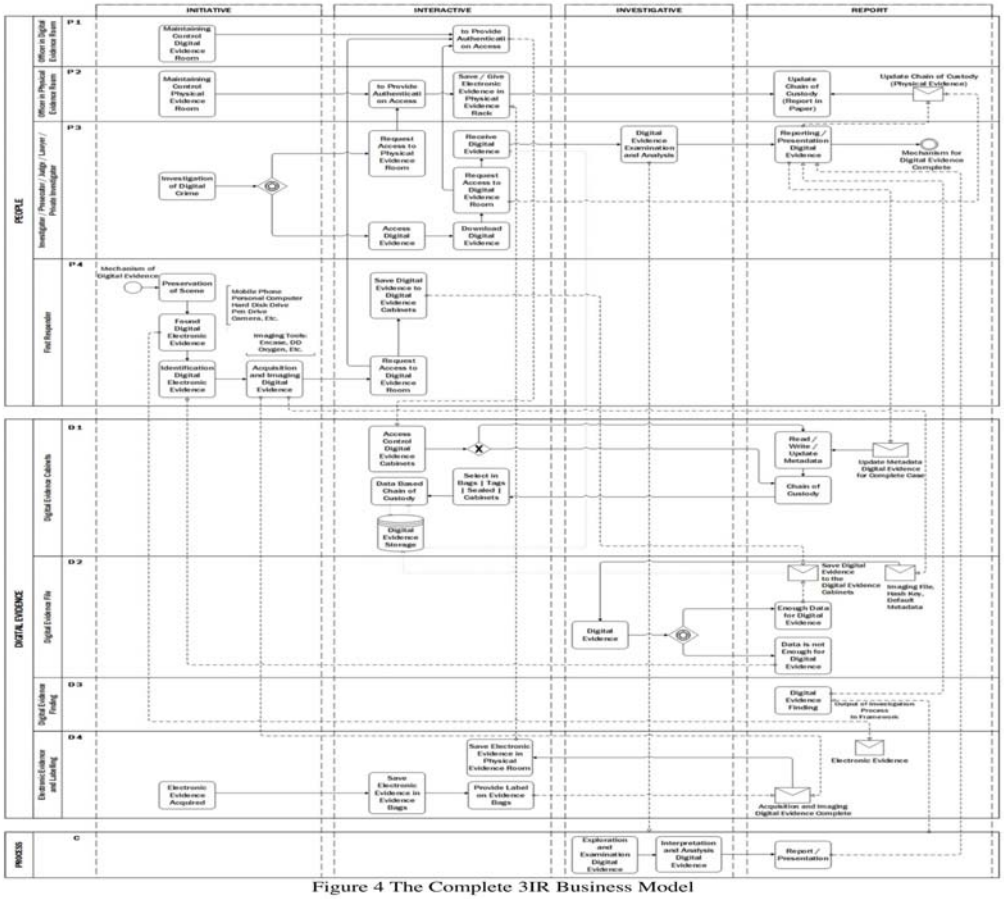

Figure 4 The Complete 3IR Business Model

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Furthermore, to test whether the model has been built correctly, then used testing through the model validation mechanism. Validation results that have been done by using Bizagi Modeller show that 3IR business model that has been built has met the validation of the provisions on bizagi modeler. In this case, the initial value of the model weighting has corresponded to the final value. Figure 3 shows the results of the validation process for 3IR Business Model using Bizagi Modeler.

Furthermore, the complete 3IR business model obtained are presented in three components, namely the People-Digital Evidence-Process as shown in Figure 4.

5. DISCUSSION

The process of developing a business model that has been implemented, trying to consider what has been described previously. In particular, it appears that investigators will be involved in the fourth phase: Initiative, Interactive, and last Investigative Report. While the First Responder will only be involved in two phases, initiative and interactive. Here is some further explanation of the 3IR business model:

- Involving three (3) components, namely: People who are involved in activities, Digital Evidence that became the main object and Process which will consist of a phase or a framework to be followed in carrying out investigative activities.
- People involved in the 3IR business model include all possible actors in the activities of digital investigation, such as first responders, forensics investigator, court, expert witness, attorney/prosecutor, judge, police officer, victim, suspect and passerby, prosecutor, lawyer/defense. In this case, based on the function and interaction with the digital evidence, then simplified into four groups: First Responder, Investigator, the officer in the physical evidence room and the officer in the digital storage room.
- The business model developed has given an overview of all activities and interactions among the parties involved with digital evidence in a whole series of phase of the investigation.
- Whatever phase of investigation used by investigators in conducting its investigation activities can be adopted by the 3IR business models.
- In the process of investigation, the 3IR business model provides an overview of how the process of obtaining digital evidence, the process of documenting, storing, accessing, and explore digital evidence and report its findings.

Meanwhile, from the standpoint of Digital Evidence shows that Digital Evidence Cabinets is a part of the digital evidence. Digital Evidence cabinets are containing interactive phase as well as the Electronic Evidence. Phase interactive on Digital Evidence Cabinets is the interaction with the system while the interactive phase of Electronic Evidence is the interaction with the physical form of electronic evidence. Digital Evidence File as a digital form of evidence is the main object of activity of the investigation, while the Digital Evidence Finding is the output of the final result. Both are grouped in phase report. Each element of Digital Evidence contained in phase report, but has different properties, the D1 (Digital Evidence Cabinets) report is in the form of record of the interaction Digital Chain of Custody, D2 (Digital Evidence File) report is in the form of metadata the basis of digital evidence, D3 (Digital Evidence finding) report is in the form of the findings of the investigation as the main ingredient of the final report. While the D4 (Electronic Evidence) report is in the form of labeling of the physical evidence.

Furthermore, for the component Process, it appears that the Process conducted after the digital evidence file obtained, then the file is used by the investigator to be explored and analyzed to obtain Digital Evidence Findings. Two phases occur in this component that is Investigative and Reports. The component Process is flexible in implementing of any digital forensics framework. In principle, any framework used by investigators will be using digital evidence as the primary object for the exploration and analysis, the final output of the component Process is digital evidence findings.

When referring to the 3IR's business model, digital forensics phase that has been widely discussed by the researchers can be classified into three groups only. The first is related to the preparation process of investigation either administrative or technical. Included in this preparation process is related to the process for the acquisition and imaging electronic evidence to obtain digital evidence. In some studies, about the framework of digital forensics, the process for the acquisition and imaging is used as the primary study. This study is driven by the fact that any electronic evidence and cybercrime cases have different characteristics, it is becoming a challenge for researchers to examine how specific techniques that can be recommended for certain electronic evidence. This is done by [38] for cloud forensics,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[39] for mobile device, [40] for network forensics. In this case, the main difference framework proposed by the researchers based on the different characteristics of the object of digital evidence. In The 3IR business model, the difference in the handling of electronic evidence and other evidence fully become part of the initiative phase.

The second group of phase is related to digital evidence analysis process to obtain digital evidence findings; then the third group is related to the reporting and presentation. The implementation of 2IR models has grouped the core of all digital forensics framework into three groups [31]. The additional phase Interactive of the 3IR models clarify the mechanism of interaction that occurs at each phase of the core digital forensics framework.

The 3IR business model can be applied to a variety of conditions that would be faced by investigator. This business model does not discuss the specifics of how the step that contains the detailed mechanisms of investigation in the form guidance of the process as a description of the phase is discussed by other researchers, but rather on the general mechanisms of how the travel of digital evidence as well as interaction with officers. A summary of the above description can be seen in Table 2.

Table 2 Multiview Business Model: Component vs Phase

Component	Initiative	Investigative	Interactive	Report
P1 : Officer in Digital Evidence Room	√	-	√	-
P2 : Officer in Physical Evidence Room	√	-	√	√
P3 : Investigator/ Prosecutor/ Judge/ Lawyer/ Private Investigator	√	√	√	√
P4 : First Responder	√	-	√	-
D1 : Digital Evidence Cabinets	-	-	√	√
D2 : Digital Evidence File	-	√	-	√
D3 : Digital Evidence Finding	-	-	-	√
D4 : Electronic Evidence	√	-	√	√
C : Process	-	√	-	√

Referring to Figure 2, it is seen that the 3IR business model can provide a snapshot of how the environment is supposed to a digital forensics activity. This business model can be described how digital evidence should be handled by the same mechanism with the physical evidence. From the discussion, the 3IR business model as a multiple view business model is an appropriate business model that required to support this mechanism. This business model is different with the existing business models or phase that is not yet able to explain the global picture of the relationship between the three principle components in digital forensics: People who run activities, Digital Evidence as the primary object and Process which serves as a guide in conducting digital forensics activities. With the explanation of the 3IR business model, then law enforcement, practitioners, and academicians can understand how it should work on the handling of physical and digital evidence.

The 3IR business models discussed in this paper is still subjective from the researcher's point of view. In this case, the regulations of the Chief of the Indonesian National Police contained in Perkap 10/2010 or Perkap 8/2014 are used as a reference in developing 3IR business model. Other regulations concerning the handling of digital evidence, such as ISO 27037, ACPO UK, NIJ USA can serve as a tool to verify the extent to which the 3IR business model has met the main needs concerning physical and digital evidence handling in the digital forensics activities.

6. CONCLUSION

The proposed 3IR as Multiview Business Model in this paper is another way to look at how the digital forensics activity should be done by law enforcement and practitioners. This is a very important concept to overcome the gaps regarding the handling of physical and digital evidence. The proposed DEC solution must be supported by the relevant business model so that the basic idea of digital evidence handling can be implemented properly.

The concept of the 3IR business model combines two aspects, first is the component involved in digital forensics activity (People-Digital Evidence-Process), the second is the phase that occurs during activity digital forensics (Initiative-Investigative-Interactive-Report). The business model describes how the environment should be present in a digital forensics activity. This concept provides an overview of the relationship between the parties who perform the activity and the relation between components in each phase of the digital forensics.

The needs of the business model are to explain some of the terms associated with a common mechanism for handling digital evidence. For example, is how the mechanisms for the management of digital evidence, how the rules of authority over digital evidence, how is a special place for the storage and recording of digital evidence, as well as how the application of transparency in the management of digital evidence. From the description of the 3IR business model it is seen that the mechanism of handling digital evidence can be explained through a combined approach of three components People – Digital Evidence - Process and 4 phase

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

investigations (Initiative – Interactive – Investigative - Process).

Through the 3IR business model can be explained anyone involved in every phase of the investigation and how the transfer of digital evidence and the interactions within each phase. This will provide a complete description than the phased approach that has been widely used by previous researchers.

Through the 3IR business model, it can be described the digital evidence handling mechanisms as well as handling of physical evidence that is handled by law enforcement. Furthermore, the concept of multiview business model proposed in this paper can be used as a reference in the future to understand how the environment is digital forensics activity and can be used as a reference for law enforcement or the practitioner involved in the activity of digital forensics.

The 3IR multiple business models have not been fully verified by digital forensics practitioners. One of the new mindsets raised in this business model is the importance of centralized mechanism of digital evidence storage. However, the limitations in network and storage infrastructure are still a consideration for being able to change the digital evidence storage mindset among digital forensics practitioners. For that, the next step that can be done as follow up of this research is to communicate and discuss with practitioners to understand the importance of applying multiple business model as part of the procedure of evidence handling in digital forensics.

In the future, this multiple business model should be supported to be implemented as a new way of viewing the handling of physical and digital evidence within digital forensic activity.

7. ACKNOWLEDGE

The research was done with the support facilities of the Department of Informatics, Digital Forensics Laboratory UII and the Laboratory of Computer Network DIKE UGM. Researchers are also grateful for the assistance of Subektiningsih in preparing the final design of the business model. This research was funded with funding support from Ristekdikti Indonesia using Doctoral Grant 2017.

8. REFERENCES:

[1] PwC, "Global Economic Crime Survey 2016," 2016.

[2] McAfee Lab, "McAfee Labs 2016 Threats Predictions McAfee Labs," 2016.

[3] D. Quick and K. R. Choo, "Impacts of increasing volume of digital forensic data : A survey and future research challenges," *Digital Investigation*, vol. 11, pp. 273–294, 2014.

[4] T. F. Gayed, H. Lounis, M. Bari, "Computer Forensics: Toward the Construction of Electronic Chain of Custody on the Semantic Web," in *The 24th International Conference on Software Engineering & Knowledge Engineering*, 2012, pp. 406–411.

[5] M. W. Beckett, "The Missing Link : Station Level Property Rooms in the Chain of Custody," *Journal of Law Enforcement*, vol. 3, no. 1, pp. 216–239, 2013.

[6] J. Richter and N. Kuntze, "Securing Digital Evidence," in *Fifth International Workshop on Systematic Approaches to Digital Forensic Engeneering*, 2010, pp. 119–130.

[7] P. Turner, "Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)," in *Digital Forensic Research Workshop (DFRWS)*, 2005, vol. 2, no. 3, pp. 1–8.

[8] B. Carrier and E. Spafford, "Getting physical with the digital investigation process," *International Journal of Digital Evidence*, vol. 2, no. 2, pp. 1–20, 2003.

[9] Y. Prayudi, A. Ashari, T. K. Priyambodo, "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia," *International Journal of Computer Network and Information Security*, vol. 7, no. 11, pp. 1–8, 2015.

[10] Y. Prayudi, A. Ashari, T. K. Priyambodo, "Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody," *International Journal of Computer Application*, vol. 109, no. 9, pp. 30–36, 2014.

[11] B. Schatz, "Digital Evidence: Representation and Assurance", Dissertation From Queensland University of Technology, Australia, 2007.

[12] A. Valjarevic, H. S. Venter, M. Ingles, "Towards a Prototype for Guidence and Implementation of a Standardized Digital Forensic Investigation Process," in *Information Security for South Africa (ISSA)*, 2014, pp. 1–8.

[13] K. Nance, B. Hay, M. Bishop, "Digital Forensics:Defining a Research Agenda," in *Proceedings of the 42nd Hawaii International Conference on System Sciences*, 2009, pp. 1–6.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[14] Y. Yusoff, R. Ismail, Z. Hassan, "Common Phases of Computer Forensics," *International Journal of Computer Science and Information Technology*, vol. 3, no. 3, pp. 17–31, 2011.

[15] A. Agarwal, M. Gupta, S. Gupta, "Systematic Digital Forensic Investigation Model," *International Journal of Computer Science and Security*, vol. 5, no. 1, pp. 118–134, 2011.

[16] M. D. Kohn, "Integrated Digital Forensic Process Model", Dissertation From University of Pretoria, 2012.

[17] R. S. Satti and F. Jafari, "Reviewing Existing Forensic Models to Propose a Cyber Forensic Investigation Process Model for Higher Educational Institutes," *International Journal of Computer Network and Information Security*, vol. 7, no. 5, pp. 16–24, 2015.

[18] S. Neuner, M. Mulazzani, S. Schrittwieser, and E. Weippl, "Gradually Improving the Forensic Process," *2015 10th International Conference for Availability Reliability and Security*, pp. 404–410, 2015.

[19] E. Casey, "Differentiating the phases of digital investigations," *Digital Investigation*, vol. 19, pp. A1–A3, 2016.

[20] S. L. Garfinkel, "Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format ," *International Journal of Digital Crime and Forensics*, vol. 1, no. March, pp. 1–28, 2009.

[21] M. M. Al-Debei, R. H. El-Haddadeh, D. Avison, "Defining the business model in the new world of digital business," in *Proceedings of the Americas Conference on Information Systems (AMCIS)*, 2008, no. 2000, pp. 1–11.

[22] A. Bock and G. George, "The Business Model in Practice and Its Implications for Entrepreneurship Research," Journal of *Entrepreneurship Theory and Practice*, vol. 35, no. 1, pp. 83–111, 2011.

[23] Č. Petar and S. Maravi, "Methodological Frameworks of Digital Forensics," in *9th International Symposium on Intelligent Systems and Informatics*, 2011, pp. 343–347.

[24] C. P. Grobler, C. P. Louwrens, S. H. Von Solms , "A framework to guide the implementation of Proactive Digital Forensics in organizations," in *International Conference on Availability, Reliability and Security*, 2010, pp. 677–682.

[25] I. O. Ademu, C. O. Imafidon, and D. S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *International Journal of Advanced Computer Science and Application*, vol. 2, no. 12, pp. 175–178, 2011.

[26] J. J. Shah and L. G. Malik, "An Approach Towards Digital Forensic Framework for Cloud," in *IEEE International Advance Computing Conference (IACC)*, 2014, pp. 798–801.

[27] Y. D. Rahayu and Y. Prayudi, "Integrated Digital Forensics Investigation Frameworks (IDFIF) Using Sequential Logic Methods," in *Seminar Nasional SENTIKA*, 2014.

[28] Ruuhwan, I. Riadi, and Y. Prayudi, "The Implementation of Integrated Digital Forensic Investigation Framework v2 (IDFIF) for Smartphone Investigation," *Journal Edukasi dan Penelitian Informatika*, vol. 2, no. 1, pp. 1–8, 2016.

[29] J. Cosic and G. Cosic, "Chain of Custody and Life Cycle of Digital Evidence," *Computer Technology and Aplications*, vol. 3, pp. 126–129, Feb-2012.

[30] G. Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," *International Journal of Computer. Science and Network Security*, vol. 11, no. 1, pp. 1–9, 2011.

[31] M. O. Hewling, "Digital forensics : an integrated approach for the investigation of cyber / computer related crimes", Dissertation From University of Bedfordshire, 2013.

[32] T. F. Gayed, H. Lounis, M. Bari, "Representing and Publishing Cyber Forensic Data and its Provenance Metadata : From Open to Closed Consumption," *International Journal of Advanced Intelligent System*, vol. 7, no. 3, pp. 662–688, 2014.

[33] P. R. Lutui, "Digital forensic process model for mobile business devices : Smart technologies", Dissertation From Auckland University of Technology i, 2015.

[34] A. Brinson, A. Robinson, and M. Rogers, "A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics," 2006.

[35] S. Perumal, "Digital Forensic Model Based On Malaysian Investigation Process," *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 8, pp. 38–44, 2009.

[36] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping Process of Digital Forensic Investigation Framework," *Journal of*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Computer Science, vol. 8, no. 10, pp. 163–169, 2008.

[37] R. Accorsi and C. Wonnemann, "Forensics Leak Detection for Business Process Models," in *Advances in Digital Forensics VII - 7th IFIP WG 11.9 International Conference on Digital Forensics*, 2011, pp. 101–113.

[38] F. Sharevski, "Digital forensic investigation in cloud computing environment: Impact on privacy," in *International Conference on Systematic Approaches to Digital Forensics Engineering (SADFE)*, 2013, pp. 1–6.

[39] Omeleze.S and H. S. Venter, "Towards a Model for Acquiring Digital Evidence using Mobile Devices," in *Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis*, 2014, pp. 173–186.

[40] S. Khan, M. Shiraz, A. W. A. Wahab, A. Gani, Q. Han, and Z. B. A. Rahman, "A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing.," *ScientificWorldJournal.*, vol. 2014, p. 547062, 2014.