I. J. Computer Network and Information Security, **2015, 11, 1-8**
Published Online October 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.11.01

A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia

Yudi Prayudi
Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia
Email: prayudi@uii.ac.id

Ahmad Ashari, Tri K Priyambodo
Department of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, Indonesia
Email: ashari@ugm.ac.id, mastri@ugm.ac,id

***Abstract*—**Digital forensics will always include at least human as the one who performs activities, digital evidence as the main object, and process as a reference for the activities followed. The existing framework has not provided a description of the interaction between human, interaction between human and digital evidence, as well as interaction between human and the process itself. A business model approach can be done to provide the idea regarding the interaction in question. In this case, what has been generated by the author in the previous study through a business model of the digital chain of custody becomes the first step in constructing a business model of a digital forensics. In principle, the proposed business model already accommodates major components of digital forensics (human, digital evidence, process) and also considers the interactions among the components. The business model suggested has contained several basic principles as described in The Regulation of Chief of Indonesian National Police (Perkap) No 10/2010. This will give support to law enforcement to deal with cybercrime cases that are more frequent and more sophisticated, and can be a reference for each institution and organization to implement digital forensics activities.

***Index Terms*—**Digital Forensics, Business Model, Investigation, cybercrime, digital evidence.

I. Introduction

According to data from PwC and RSA as cited by [1], cybercrime has transformed into a serious threat that value of losses globally could reach national revenue of a country. This is in line with a report from [2] who revealed that cybercrime is the industry that grows from year to year with the high rate of return but with little risk. Meanwhile, according to [3], although there is no official definition of cybercrime, for the sake of practicality, cybercrime can be defined as "*a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations*". Meanwhile, [4] argues that cybercrime is not a new crime, but rather classic crimes exploiting the computing power and accessibility to information. According to [4], Cybercrime is a consequence of excessive availability and user proficiency of computer systems in unethical hands.

Besides supported by the increasing of various electronic and information technology equipment, according to [5], the rising of cybercrime industry is supported by blackmarket, that is, industry where various parties can interact economically for anything related to services, tools or infrastructure that can be used for conducting cybercrime. With the blackmarket, cybercrime activities and the data generated become more difficult to identify because the activities involve many parties. This has an impact on the handling process of cybercrime, more complicated and requires updated analysis techniques.

Furthermore according to Agarwal in [1], the handling of cybercrime case are conducted through investigation activities known as digital forensics. According to [6], digital forensic is "*the procedure of investigating computer crimes in the cyber world*". Agarwal in [1] also mentioned that digital forensics is the use of science and methods for finding, collecting, securing, analyzing, interpreting, and presenting digital evidence for the sake of reconstruction and validity of judicial process. On the other hand, Palmer [7] suggested the initial definition of digital forensics as "*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*."

Forensics itself is the implementation of scientific methods or the application of structured steps to assist the process of an investigation carried out by law enforcement. Thus, digital forensics is a structured step in the process of investigating and handling evidence to minimize the presence of errors in the investigation process [8]. Furthermore, for each activity in the digital forensics to be classified as a scientific method, this can refer to certain structured steps, known as the term of a framework. Peter and Maravi [9] states that the

framework is "*a structure to support a successful forensic investigation"*. In the field of digital forensics, the structured step is often known with some terms: framework, methodology, forensics process or stages.

According to [4], the development of a methodology in digital forensics that encompasses the forensic analysis of all genres of digital crime scene investigations is the most crucial part in law enforcement activities. In this case, the investigators must employ consistent and well-defined forensic procedures.

The increasing of the complexity of cybercrime provides challenges and opportunities towards research in the field of digital forensics. In this case, according to [10] one of the important keys for improving research is the availability of compassable models for forensic processing.

Digital forensics activities will involve many people. According to [11], digital forensics activities will engage a number of people with different roles such as *first responder, forensics investigator, court expert witness, attorney, judge, police officer, victim, suspect and passerby*. It supposes to depict the interaction among the officers and their interaction with digital evidence in a whole series of the investigation process. The business model approach can be suggested to show the interaction in question.

For example, [12] has given the proposed frameworks for digital forensics analysis derived from a different source of digital evidence. Fig 1 shows the frameworks proposed by[12]. However, on the proposed frameworks, there are some things that are not yet clear, for example, who run those frameworks, how does the storage mechanisms of digital evidence obtained, how is the access mechanism to the digital evidence being analyzed. The same thing also happened with the proposed frameworks presented by other researchers.

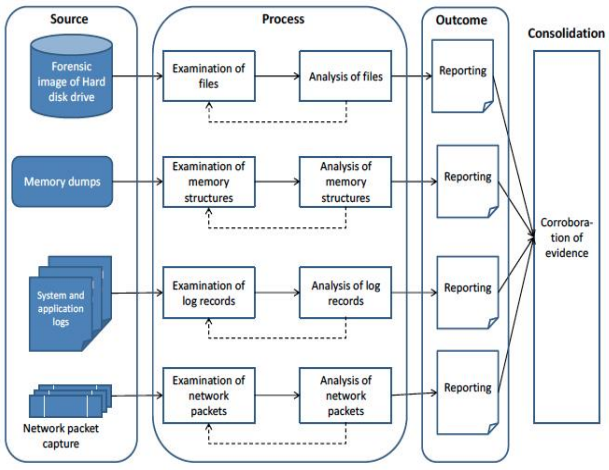

Fig.1. Digital Forensics Analysis on Different Sources From [12]

In the context of digital forensics, the business model will depict the linkages between the person conducting the activity, the relationship between each stage in the frameworks, and the role and position of each person and object involved. The differences in business model will cause differences in the overall handling of digital forensics activity, including the handling of digital evidence and chain of custody. Unfortunately, among digital forensics practitioners, there has been no study resulted, concerning the issue of business models in digital forensics and how to implement the models in daily practice. In this case, what has been resulted by [13] through business models of the digital chain of custody can be made as an initial step to develop business models of digital forensics.

The business model approach in understanding digital forensics activity will hopefully raise deeper understanding of the whole and complete process of digital forensics. This will eventually give support to law enforcement in handling cybercrime cases, which become increasingly more sophisticated. Also, the availability of studies about digital forensics business models will give references for each institution and organization carrying out digital forensics activities.

II. Previous Works

The literature review indicates there is a wide variety of frameworks, methodology or stages to be followed in carrying out digital forensics activities. Varying frameworks for digital forensics in fact are not much different principally because in general, any framework that has been mentioned by the researchers show only slight differences in terms of naming and details of digital forensic activity [14]–[16]. The framework discusses only the stage, methodology or investigation model that can be applied in implementing digital forensics activities. Among the frameworks are Generic Computer Forensic Investigation Model (GCFIM) proposed by [17], The Four Tier Model from [15], Integrated Digital Forensic Process Model (IDFPM) from [18], as well as Integrated Digital Forensics Investigation Framework (IDFIF) from [19]. Meanwhile, [20] also proposed a framework for digital forensics with the approach of an organizational investigative model.

The author himself [21] suggests the general model and the conceptual model of digital forensics in the notation below:

$$\text{General Model DF} = \{I, S, D, E, A, R\} \quad (1)$$

I = Identification process,
S = Storage for digital evidence,
D = Documentation of digital evidence,
E = Exploration,
A = Analysis data and
R = Reporting

$$\text{Conceptual Model DF} = \{Pi\ [Tj, Lk], DE\} \quad (2)$$

Pi = A series of digital forensics process,
Tj = Technique, methods, approach, system, tools.
Lk = Legal principle,
DE = Digital Evidence

Based on earlier descriptions and notations of the

general and conceptual model, a discussion of methodology, or framework stages in digital forensics is conducted from the perspective of a digital forensics examiner or investigator. 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.

Digital forensics will always include at least all of these 3 (three) components: (1) human who conducts the activity, (2) digital evidence as the main object, and (3) the process as a reference for the activity to be followed. The terms of methodology, frameworks, or digital forensics stages tend to put forward the third aspect only. The existing frameworks have not described how the interaction between human, interaction between human and digital evidence, and interaction between human and the process itself.

The author himself in the paper about digital evidence cabinets have tried to develop a preliminary model of the business model for the handling of digital evidence [1]. The business model is needed as a foundation for solutions to the problems of the digital chain of custody in the form of digital evidence cabinet. Nevertheless, these early models need to be clarified the function and its role in the general scheme of digital investigation.

III. Review of Digital Forensics Framework

As [22] suggested, digital forensics are regarded as a new form of forensic science, and it is a field of science that is still potentially growing, yet has not shown itself as an established field of study when compared to the other forensic field, especially when compared with forensic medicine. In this case, the use of fingerprint and DNA in the field of forensic medicine appears to be the real contribution of forensics in support of criminal investigation processes.

One of the obstacles found in the digital forensics field is that the contributions of the practitioners are still more dominant compared to the contributions of the researchers. Therefore, [23] argued that the methods and processes that serve as references in a digital investigation process are generally *investigator based*, and also depend on personal experience and expertise, and it is casuistry in nature or so-called ad hoc basis. This is in line with the opinion of [24] that scientific development of digital forensics is characterized with practitioner-driven nature.

Kruse and Heiser in [9] suggested that, although there are many opinions about the methodology in digital forensics, generally those can be summarized in the acronym of 3A, namely:

- Acquiring, getting digital evidence with emphasis on data integrity principle,
- Authenticating, validity of data throughout the investigation process is in accordance with the original digital evidence retrieved from the acquisition process,
- Analyzing, the process of obtaining relevant data to remain attentive to the authentication and integrity of digital evidence.

While according to Carrier and Spafford in [7], the framework of digital investigation must be according to the purpose, not the stage or task. It is worth noting, given every institution has certain uniqueness, and each case has its characteristics. Therefore, if the methodology is based on the stage or task, it is very possible to raise differences between institutions, likewise between cases that are being handled. Thus Carrier and Spafford put more emphasis on the application of the objective-based framework, not task-based.

Some researchers have tried to discuss and do a comparison against some framework of the digital investigation. In this case, [25] trying to do an analysis of some of the previous framework as well as explain the advantages and disadvantages of each framework. The analysis is performed with the focus on an implementation in a higher educational institute. While [17] also did an analysis of some of the frameworks then simplified it into a Generic Computer Forensic Investigation Model (GCFIM). A similar thing is done by [19] by conducting an analysis of some existing framework, then provide a new model using the sequential logic approach to generating IDFIF.

Meanwhile, other researchers provide solutions to digital forensics frameworks for a number of different specific environments, such as [26] which gives the solution frameworks for the problem of web security attack, [16] provides a framework solution for cloud computing environments, [27] gives the proposed framework related to wireless cybercrime cases. Digital forensics frameworks that have been developed by the researchers according to [10] rely on the ability to make the best use of digital evidence that is found.

Meanwhile, the increasing use of a wireless network, have also had an impact on the increasing cases of wireless cybercrime. The use of wireless known as a new way of Internet connections and lead to the emergence of a new crime patterns. In this case, [27] has proposed the Digital Forensics Standard Operating Procedures for Wireless Crimes.

A large number of framework and investigation model turned out to be a problem. Every researcher and the institution can propose or develop its framework. This is certainly going to lead to the absence of a standard that can be used as a reference for all the institutions that run the digital forensics activity. It needs an effort to unify and summarize all investigation models. In this case, [28] has provided the solution through the concept of harmonized digital forensic investigation process model.

IV. A Proposed Business Model for Digital Forensics

Based on the experience of interacting with digital forensics practitioners, both in law enforcement institutions as well as non-law enforcement institutions

(such as public accounting and auditing office, private investigator), the business model according to the practices in the handling of digital evidence can be illustrated in Fig 2.

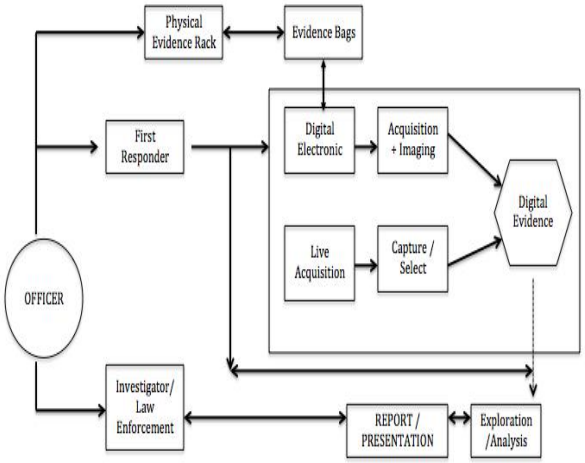

Fig.2. Illustration of the Business Model based on Actual Practices of Digital Evidence Handling

The illustration in Fig 2 has been involving 3 (three) components as previously described, namely: human, digital evidence, and process. From that figure, raise an important issue in digital forensics, i.e. unavailability of storage method and recording of a chain of custody of digital evidence. In regards to The Regulation of Chief of Indonesian National Police (Perkap) No 10/2010, both aspects play a pivotal role in handling evidence. Thus, it can be concluded that the practices of digital forensics currently are still not fully in compliance with the provision stipulated. It is required improvement on the illustration in Fig. 1 to construct a business model that complies with the provision of The Regulation of Chief of Indonesian National Police (Perkap) No 10/2010.

According to [29], a business model is "*an abstract representation of an organization*". While based on the idea suggested by [30], the term of business model is commonly used to represent the main aspects of a business. A business model can be conceptual, textual or graphical that show the connectedness, cooperation or planning of all components involved, in accordance with the core business of the institution in order to achieve the goals set by the institution.

In these research, to build a business model for digital forensics, the steps to follow are:

a. Identifying the main purposes of digital investigation in the area of law enforcement. In this case, prosecution after the fact/scene of illegal activities is the main purposes of the digital investigation [20].
b. Identifying basic principles held as a reference for the handling of evidence. As what has been argued by [1], *The Regulation of Chief of Indonesian National Police (Perkap) No 10/2010* can be cited as a reference on the general principle of handling evidence [31].
c. Identifying the object involved in the digital forensics activity. In this case, the objects of digital forensics activity are: *human* (first responders, officers who manage the storage, investigator, and others), *digital evidence* (electronic evidence, process of getting the digital evidence, evidence storage, and access to evidence) and *process* (phases for exploration, analysis, report and presentation).
d. Recognizing the environment and how the digital forensics activity works. For such reason, the environment and method of digital forensics can be illustrated in Fig 3.
e. Constructing a business model that explains the linkages between objects in the work environment of digital forensics. Fig 4 shows an illustration of the proposed business model that can be used within the scope of digital forensics.

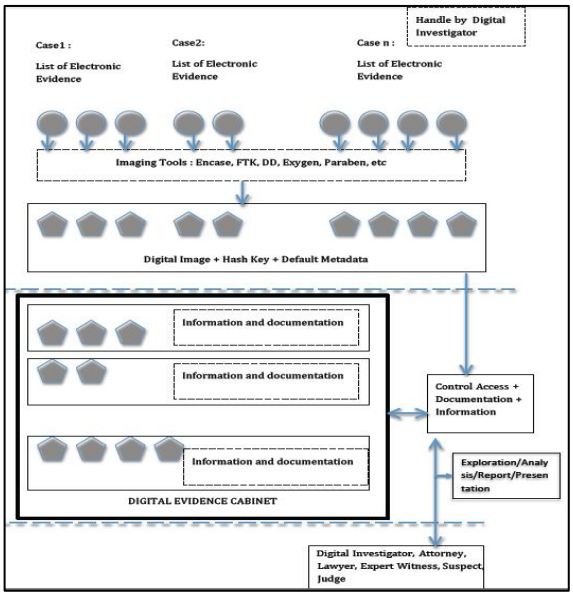

Fig.3. The Conceptual Method of Digital Forensics Activity

In developing a business model of digital forensics activity, then given a technical definition and basic assumptions as follows:

a. Digital evidence is an output resulting from the acquisition or imaging process of electronic evidence. The process can be done using either offline or online technique. This output becomes the primary source for exploration, analysis and interpretation of the data that will support investigation process of a scene.
b. As physical evidence, digital evidence is also supposed to be stored in a special storage place. Therefore, the basic assumptions of the business models that will be built are referring to the concept of Digital Evidence Cabinets where all digital evidence stored in a storage area. Investigator or law enforcement agencies will do the control mechanisms to be able to access the digital evidence.

Based on Fig. 4, the business model will be divided

into three groups of activities. The first group is the interaction between people with evidence for early handling of digital evidence. The second group are the activities for the implementation of the chain of custody as a mechanism for recording and documentation, access to digital evidence. While a third group is a main activity, namely conducting exploration, analysis and presentation of findings. There is three main mechanisms in the business model, the initial mechanism for the handling of digital evidence, a mechanism for recording and storage of digital evidence as well as the mechanism for analysis of digital evidence. All the mechanism shows how the relationship between the three components described earlier namely people, digital evidence and process.

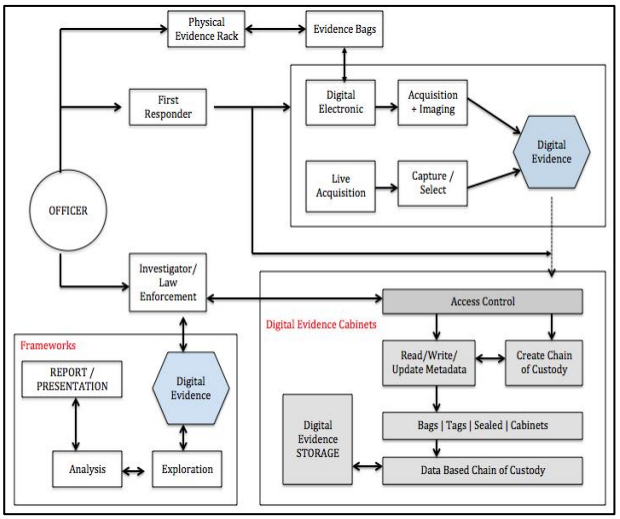

Fig.4. Proposed Digital Forensics Business Model

V. Discussion

According to [32], the majority of countries in the world does not yet legally distinguish electronic evidence from physical evidence. Even some countries have not accepted electronic evidence altogether in its legal system so that an attempt to perform an investigation and verification of cybercrime cases cannot entirely be handled by law enforcement. Therefore, it is reasonable that the study about the business model of digital forensics is still very limited or even has not yet become a major concern in the scope of digital forensics activities.

Meanwhile, [1] argued that in handling a case, both physical evidence and digital evidence are part of the investigation process that complement each other. Similarly, at the time of the trial, both physical evidence and digital evidence become a unity in the process of investigation. Thus, the handling of physical and digital evidence must be the same, or at least have a similar mechanism. This can be illustrated by [33] as in Fig 5. The model is the development of a similar issue delivered by [20] but with a slightly different model. In his opinion, [20] explains that there are five main phases, i.e., readiness phase, deployment phase, physical crime scene investigation, digital crime scene investigation and review phase. In this model, the physical and digital phases feed into each other in terms of locating potential sources of evidence.

Unfortunately, the scheme illustrated in Fig 5 does not appear in the studies about the stages and methodology of digital forensics. Moreover, based on the literature study presented by [9], [34]–[36], the focus is still on stages of digital forensics activity rather than on the interaction between actors and digital evidence involved in the digital forensics activity, or an overview of the importance of unity in handling physical evidence and digital evidence. Therefore, the proposed business model in this paper will include the point of view of digital forensics activity that focuses on the interaction between actors and digital evidence.

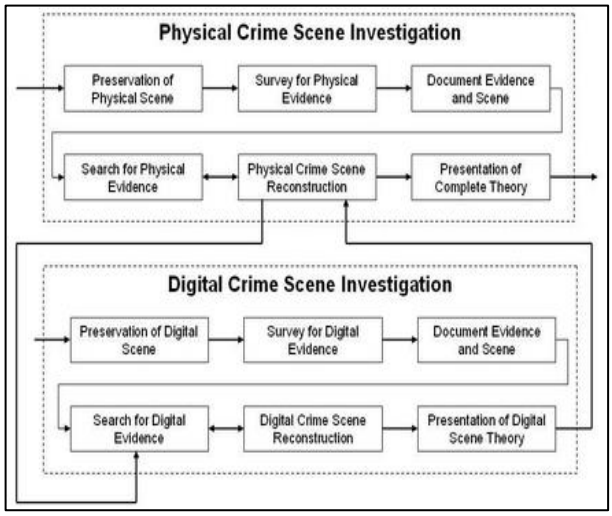

Fig.5. An Illustration of Unity in Handling Physical and Digital Evidence From [33]

As what [11] revealed, a digital forensics activity involves a number of people, namely *first responder, forensics investigator, court expert witness, attorney, judge, police officer, lawyer, victim, suspect, and passerby*. To that end, the proposed business model in this study has involved activities from at least 3 parties, namely: first responder, police officer in the storage room, and law enforcement as the party involved in the investigation process that consists of forensics investigator, court expert witness, attorney, judge, and lawyer.

In Fig 4, it is obvious that three elements involved in digital forensics activity, i.e., first responders, officer, and law enforcement. The business model also gives a description of how digital evidence should be kept and used for the purposes of the analysis in the case investigation. The illustration in Fig 4 also provides an overview of how to apply the principle of unity in the handling of both physical and digital evidence as described by [33].

In addition, the proposed business model in Fig 4 generally has met the principles of a business model as explained by [29], namely representing the main aspects of an activity in graphics and describing the connectedness among components involved in

accordance with the core business of the institution. For this sake, the goal to be achieved is how to run a digital forensics activity in accordance with the principle of law enforcement while remaining attentive to the characteristics of the handling of digital evidence in cybercrime cases.

From the description in the introduction, it is mentioned that digital forensics activities will always involve at least 3 (three) components, namely: human conducting activities, digital evidence as the main object, and process as a reference for the activities to be followed. It also has been stated that the term of digital forensics frameworks tends to discuss only the third aspect. The existing frameworks have not clearly depicted the interaction among humans, between human and digital evidence, and between human and the process itself. Therefore, the business model proposed in this study depicts another point of view in describing digital forensics activities with a focus on the human involved, as well as the available digital evidence. While aspects of frameworks/methodologies/stages are part of the stages in digital evidence analysis.

The need for a business model is driven by various interpretations of digital forensics activities in the field, particularly in the sphere of law enforcement in Indonesia. Given the importance of the handling of digital evidence as part of the effort of case disclosure in cybercrime, the need for a business model of digital forensics also will be more conveniently located. The handling of digital evidence is not only regarding the mechanism of the framework/methodology/stages, but should also consider the interactions of all objects involved in a digital forensics activities. Unfortunately, this still has not been brought to the attention of the parties that are practically involved in activities of digital forensics. Thus the input of business model proposed in this paper can be used as a reference for understanding the environment in digital forensics activity and can serve as a reference for law enforcers or practitioners engaged in digital forensics activities.

Admittedly, there is a gap between the current real practices and the proposed business model. The gap is, especially in terms of how to store and maintain the digital evidence. Referring to Figure 2, the actual practice of storing digital evidence is still in the form of hard disk that contains imaging results of and then is given a specific label for later stored on shelves that physically contain the hard disks as the results of the imaging process. This is in contrast with the concept of the business model proposed, that digital evidence should be stored in the form of digital files and kept in the main storage. This gap is based on the fact that the process of acquisition and imaging is practically easier to do directly on the media hard disk. Also, the process requires very large storage capacity. If this is done through the conventional file transfer mechanism, certainly it will be time-consuming and require very large bandwidth capacity.

It is clear that there are some gaps between actual practices and the proposed business model. However when it refers to The Regulation of Chief of Indonesian National Police (Perkap) No 10/2010, indeed the proposed business model is a description of the handling of digital evidence that is relevant with similar things which are done conventionally. Even though there is currently a gap between the actual practices and the business model proposed, in line with the development of transfer technology and data storage, the perceived barriers in implementing the business model will someday be resolved. Thus, the proposed business model is still very relevant to serve as a reference in understanding the environment of digital forensics activities.

Compared to the findings of previous studies through the business model of the digital chain of custody [13], the proposed business model of digital forensics in this study is a kind of extension of the previous model. In this case, the extension is that the business model of a digital chain of custody is one of the details of activities in human interactions with digital evidence, particularly in terms of documentation of the interactions.

The proposed business model in this paper is based on the viewpoint of law enforcement. In this case, Forrester [20] argue that digital forensics purposes are different between law enforcement with a military as well as business and industrial. The difference can be seen as in Table 1. Forrester himself in his paper has explained the details of the differences of digital forensics purposes in each of these areas.

Thus, a business model that is applied will have different characteristics between the viewpoint of law enforcement with a military as well as business and industrial. For that reason, then one open problem that can be set as the next area of research is how to build a digital forensics business models that are relevant to the area of military as well as business and industry.

Business models that have been proposed in this paper are based on assuming the early existence of a prior incident activity that then requires a digital investigation. This contrasts with the military and business or industry areas where digital forensics activity does not always have to be based on the existence of a prior incident activity. In this case for the areas of military, business and industry, the activities of digital forensics are closely connected with the issue of computer security.

Table 1. Investigation Objective From [20]

Area	Primary Objective	Secondary Objective	Environment
Law Enforcement	Prosecution	-	After The Fact
Military	Continuity of Operations	Prosecution	Real time
Business and Industry	Availability of service	Prosecution	Real time

VI. Conclusion and Suggestion

This paper has discussed the importance of digital forensics activity in the handling of cybercrime cases.

The increasing number of cybercrime cases should be followed by the more authoritative institution that runs digital forensics activities. In this case, one thing perceived as a weakness in the institution is the absence of a description of the relevant business model to depict how digital forensics activities should be run. The existing study of the literature is more focused on aspects such as framework/methodology/stages, while the interaction between human and digital evidence has yet to be fully seen.

The proposed business model already accommodates major components of digital forensics (human, digital evidence, process) and considers the interactions of the components. The business model also contains several basic principles in compliance with The Regulation of Chief of Indonesian National Police (Perkap) No 10/2010. Although in practice the proposed business model does not match with the actual practice, it is more on the technical constraints faced by practitioners/digital investigator in implementing digital forensics activities truly in accordance with the regulation set forth.

The proposed business model principally is an extension of previous efforts done by the author to build the business model of a digital chain of custody. Through the extension of the business model approach that has been proposed, it is expected to provide a whole and deeper understanding against the digital forensics process. This will support law enforcement in dealing with cases of cybercrime, which are becoming more sophisticated.

Future research that can be done is to identify the infrastructure that will support the implementation of the business model of digital forensics that has been proposed in this paper. The next step to do is to conduct socialization and further discussions on various forums for digital forensics practitioners or academics to get better input for the concept of digital forensics business model.

REFERENCES

[1] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody," *Int. J. Comput. Appl.*, vol. 109, no. 9, pp. 30–36, 2014.

[2] CSIC, "Net Losses : Estimating the Global Cost of Cybercrime," Washington DC, 2014.

[3] N. Kshetri, *The Global Cybercrime Industry*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[4] M. R. Clint, M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensic Models," *Int. J. Digit. Evid.*, vol. 1, no. 3, pp. 1–12, 2002.

[5] L. Ablon, M. C. Libicki, and A. A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," Santa Monica USA, 2014.

[6] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani, and F. Daryabar, "Digital Forensic Trends and Future," *Int. J. Cyber-Security Digit. Forensics*, vol. 2, no. 2, pp. 48–76, 2013.

[7] N. L. Beebe and J. G. Clark, "A hierarchical, objectives-based framework for the digital investigations process," *Digit. Investig.*, vol. 2, no. 2, pp. 147–167, 2005.

[8] E. K. Mabuto and H. S. Venter, "State of the art of Digital Forensic Techniques," in *Information Security for South Africa (ISSA)*, 2011.

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

[10] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digit. Investig.*, vol. 7, pp. S64–S73, Aug. 2010.

[11] 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.

[12] S. Raghavan and S. Raghavan, "The Digital Forensic Landscape," *SecureCybers*, pp. 1–9, 2012.

[13] Y. Prayudi, A. Luthfi, and A. M. R. Pratama, "Pendekatan Model Ontologi Untuk Merepresentasikan Body of Knowledge Digital Chain of Custody," *Cybermatika ITB*, vol. 2, no. 2, pp. 36–43, 2014.

[14] C. P. Grobler, C. P. Louwrens, and 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.

[15] I. O. Ademu, C. O. Imafidon, and D. S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 12, pp. 175–178, 2011.

[16] 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.

[17] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases of Computer Forensics," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 17–31, 2011.

[18] M. D. Kohn, "Integrated Digital Forensic Process Model," no. November, 2012.

[19] Y. D. Rahayu and Y. Prayudi, "Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic," in *Seminar Nasional SENTIKA*, 2014.

[20] J. Forrester and H. Building, "A Digital Forensics Investigative Model for Business Organizations," in *Proceedings of the ISSA 2006, Insight to Foresight Conference*, 2006, pp. 1–12.

[21] Y. Prayudi and Azhari, "Digital Chain of Custody : State Of The Art," *Int. J. Comput. Appl.*, vol. 114, no. 5, pp. 1–9, 2015.

[22] P. B. Turner, "Digital Evidence Bags," Oxford Brookes University, 2008.

[23] A. Valjarevic, H. S. Venter, and 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.

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

[25] R. S. Satti and F. Jafari, "Reviewing Existing Forensic Models to Propose a Cyber Forensic Investigation Process Model for Higher Educational Institutes," *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 5, pp. 16–24, 2015.

[26] A. Lazzez and T. Slimani, "Forensics Investigation of Web Application Security Attacks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 3, pp. 10–17, 2015.

[27] I. L. Lin, Y. S. Yen, and A. Chang, "A study on digital forensics standard operation procedure for wireless cybercrime," *Proc. - 2011 5th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2011*, vol. 2, no. 3, pp. 543–548, 2011.

[28] A. Valjarevic and H. S. Venter, "Harmonised digital forensic investigation process model," *2012 Inf. Secur. South Africa*, pp. 1–10, 2012.
[29] M. M. Al-Debei, R. H. El-Haddadeh, and 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.
[30] A. Bock and G. George, "The Business Model in Practice and Its Implications for Entrepreneurship Research," *Entrep. Theory Pract.*, vol. 35, no. 1, pp. 83–111, 2011.
[31] Kepolisian Negara RI, "Perkap Tata Cara Pengelolaan Barang Bukti," Jakarta, 2011.
[32] UNODC, "Comprehensive Study on Cybercrime," New York, USA., 2013.
[33] B. Carrier and E. Spafford, "Getting physical with the digital investigation process," *Int. J. Digit. Evid.*, vol. 2, no. 2, pp. 1–20, 2003.
[34] S. Perumal, "Digital Forensic Model Based On Malaysian Investigation Process," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 8, pp. 38–44, 2009.
[35] M. Kohn, "Framework for a Digital Forensic Investigation," in *ISSA Computer Security*, 2006, pp. 1–7.
[36] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping Process of Digital Forensic Investigation Framework," *J. Comput. Sci.*, vol. 8, no. 10, pp. 163–169, 2008.

Authors' Profiles

Yudi Prayudi, Currently he is a Ph.D Student at The Department of Computer Science and Electronics Gadjah Mada University and also a senior lecturer at Department of Informatics Universitas Islam Indonesia Yogyakarta, Indonesia. His research interests include digital forensics, cybercrime, watermarking, steganography, malware analysis and network security.

Dr. Ahmad Ashari, Currently he is an Associate Professor at The Department of Computer Science and Electronics Gadjah Mada University. His research interests include Computer Network, Distributed System, Pararel Computation and Web Technology.

Dr. Tri Kuntoro Priyambodo, M.Sc., currently he is an Associate Professor at Department of Computer Science and Electronics Gadjah Mada University. He is a member of IEEE. He is also hold a position as a Secretary of Satellite and Aerospace Electronics Research Group, Gadjah Mada University. His research interests include Computer Network Security, eGovernment Systems, and Autonomous Unmaned Systems.

How to cite this paper: Yudi Prayudi, Ahmad Ashari, Tri K Priyambodo,"A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia", IJCNIS, vol.7, no.11, pp.1-8, 2015.DOI: 10.5815/ijcnis.2015.11.01