International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(2): 106-110
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)

Improvising the Input Process of Traceability Model for Digital Forensic Investigation

Iman Ahmeid Mohamed
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
eman_ahmeid@yahoo.com

Azizah Bt Abdul Manaf
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
azizaham.kl@utm.my

***Abstract*— In this paper, we present an enhancement input in the traceability model of digital forensic investigation. Plus, we present a literature review about existing traceability models. Furthermore, the outcome of this model expected to help and improvise the traceability model with theoretically proven justifications.**

Keywords—Forensic, traceability, Scenario, Evidence

I. INTRODUCTION

Today's world has a large growth of technology in increasing numbers of computers, portable devices and networks, Due to such growth, criminals are becoming smarter and trickier to trace, which makes it easier to commit crimes and fulfill an illegal purpose. However, digital forensics come in finding a way to handle the increasing amount of digital crimes by carrying out certain procedures and processes to track the source of the crime through finding evidence to uncover the identity of the offender. Therefore, a lot of people are exploring this field worldwide and such procedures continuously evolve.

According to RSA 2012 cybercrime trends report review, cybercrime is constantly displays no signs of reducing down. In fact, 2011 noticeable a year of new advanced risks and threats, as increasing the level of sophistication in the attacks testified and witnessed around the world. As we moved into 2012, cybercrime is diverging down with a different direction as new financial malware and viruses variants emerge, cybercriminals find new way to monetize non-financial data and the increasing of hacktivism-related inhales new life into an old adversary [1].

On the whole, in this research paper we are focusing on tracing the evidence using traceability model. The input process of the traceability model will be enhanced by adding a significant phase to make the model work effectively.

II. Issues in Digital Evidence

In [2] has been stated that, because of the higher amount of information that can be obtained from a forensics investigator, it needs to examine the ethical consideration, in order to use this information to prosecute a legal act and to prevent reduction during the trial, evidence must be gathered effectively and lawfully. It is particularly important to be conscious about the privacy rights of suspects, victims and uninvolved third parties. Any person challenge to examine such a case should be acquainted with the primary technological innovation involved in collecting the information, how to effectively gather the data, and how to ensure that the information will be legitimate as evidence during trial.

There are many reasons for the unsolved digital crime cases; one of the reasons could be not conducting the forensics investigation steps to find the evidence. Gathering the evidence should have the proper tools to complete the process while having the skillful investigators required to collect the evidence. Another point is that, in the prosecution will identify that the case is not solved due to not compiling the necessary steps to prove the evidence collected. The criminals are highly knowledgeable about the forensics; meanwhile they struggle to hide themselves in a very professional way. In addition to that, the organization may lack the tools or the skillful people to gather the evidence [3].

Thus, the issues highlighted in [4] can be summarized in the following points:

- Disorganization of the evidence For instance, a hard drive platter contains many pieces of information mixed together and layered on each other over time.
- The abstraction of the digital incidents that gives a partial view of what occurred in each crime occurred.
- Intentionally alteration or manipulation of the digital evidence without leaving any traces.
- The complexity of the methods of computerized evidences and traditional evidences, where traditional evidences are generated and retrieved as a single record but in computerized evidence, it is generated or retrieved from different records and sources.

III. DIGITAL FORENSIC

Digital Forensic can be described as the process of using techniques and methods that are forensically approved to collect, preserve, analyze and document the digital evidence to present the original source in the court [5]. Therefore, digital forensics has persisted as long as computers and digital devices have stored data that could be used as evidence. Thus, digital forensic was performed by government agencies, but has become common in the commercial and other sectors over the past several years.

IV. TRACEABILITY IN DIGITAL FORENSIC INVESTIGATION PROCESS

Generally, traceability is very significant phase during the digital evidence investigation process, which is the key used in forming and identifying the chain of evidence. Traceability is a broad and an instrument that attain many different objectives to finish the tracing process which is very complex. Moreover, [5] defined traceability as the approach that trace and map the evidence to find the source of the incident.

Traceability of the digital evidence process becomes very necessary in investigation aspects as it is applicable to track the different sources of the evidence. Cyber crimes or digital crimes are now serious, extensive, competitive, increasing and progressively innovative, which poses major effects for nationwide. However, there are challenges that investigators face during acquiring and tracing the digital evidence as follow:

- Lack of traceability models that is used for digital forensic process as well as a limited number of research about it.
- Hard to deal with the function of the traceability model, that is to say, difficult to comprehend and uneasy to identify the process of tracing where it is used as theoretical base.

However, traceability in digital forensic investigation process has been addressed in [5] as the process of finding the original source that caused the incident. The traces can be found in electronic devices as well as digitally examining the activities such as in network, whereby it needs to identify the open ports, protocols numbers and the IP addresses associated to the source of the incident. Besides that, it can be on database documents or internet activities, to be able to construct trace pattern that enables the investigator to find the source of the incident during the digital investigation process [6].

V. TRACEABILITY MODELS

This section provides a summary of the researches that propose traceability models in various areas.

A. A conceptual Model of Traceability of Safety Systems

The model is needed as an initial solution that is generating traceability approach for traceability management of safety system. It gives an overview of the data produced during development, safety analysis process and the relation between those data. However, the traceability has a direct effect on the success of system implementation, due to the lack of good methods and tools to provide additional personnel resources. It has declared the necessity of developing a traceability model for safety systems. The approach developed to be used to capture and maintain traceability as well as performing impact analysis. The two main reasons of developing the traceability approach were to trace such hazards, safety requirements to the design and implementation. Moreover, it is stated that there are two sets of traces need to be developed which are solved in the safety system, which are, firstly, Development, maintenance and testing (requirements). Secondly, the safety analysis and certification which is applied by providing proof of conformance method [7].

B. Model-Based Traceability

The model-based traceability propose an approach by establishing traceability matrices that helps project stakeholders in the organization to prepare, produce and perform traces in graphical modeling environment.. The model aims to manage traceability strategies and queries, and thus introduce four layered model for defining traceability metagraph. It could help the stakeholders to plan, generate and execute trace strategies in modeling environment [8].

C. Research for Traceability Model of Material Supply Quality in Construction Project

The traceable model is designed for the quality of material content. It built the content supply quality for project development. It traces the quality of the material content and then validates and proves the project development. The system achieves the tracking and tracing of material quality in supply chain. Then, through the instance of application, validity and feasibility of the model will be proved [9].

D. Traceability between Software Architecture Models

The framework is to record and trace the data between software architecture models using traceability model to help developers comprehend the software system lifecycle as well as understanding the reason of occurring on modification and renovation of designing the traceability model. With the traceability approach or model, one can trace back to find out the information due to the relative simplicity of high level software architecture models [10].

E. A model for requirements traceability in a heterogeneous model-based design process: Application to automotive embedded systems

The model is used for real time design for requirement traceability, whereby, it contains validation and verification on the model activities to ensure the coordination of the preliminary requirements of particular product. The model establishes a link between these flows and affords full traceability of requirements, including those set for heterogeneous models based on application to automotive embedded systems [11].

F. Adapting traceability in digital forensics process

The proposed model called traceability model that uses in digital forensic investigation process, to trace pattern of the original source of an incident. The purpose of the model is to ensure the accurateness and completeness of the traces found and the relationship between them. The model is to illustrate the relationship in the digital forensic investigation process by integrating the traceability features. Moreover, the model is to trace and map the evidence to the source and shows the link between the evidence, the entities and the sources involved in the process [6].

VI. SUMMARY OF TRACEABILITY MODELS

As mentioned, traceability is a broad approach and it can be applied in many fields and purposes such as software system development. In fact, as a review of the traceability models, we can notice that traceability researches concentrated on traceability of design, implementation of the requirement such as architecture design. However, as we have reviewed the traceability models, it can be said that each model serves a different purpose, but they all fall under traceability approach. It means, most of the models are used to trace the requirements of the development or software system to ensure its functionality, well- implemented and accurate design.

On the other hand, the traceability model for digital forensic investigation process is only proposed by (Siti Rahayu Selamat & Robiah Yusof & Shahrin Sahib& Irda Roslan &Mohd Faizal Abdollah& Zaki Mas'ud – 2011). on the work done in the paper "Adapting traceability in digital forensics process" [6]. It is considered as the only and recent paper that uses traceability in digital forensics investigation.

VII. TRACEABILITY MODEL OF DIGITAL FORENSIC INVESTIGATION PROCESS

The model discusses what kind of information such as object that represents characteristics of the information. The object is showed with the link named traces to in the traceability model to describe that the stakeholder has a role in tracing the object. Furthermore, stakeholder describes the persons involved in the traceability process with different roles such as investigator, complainer or administrator. The source describes the original location of the traced information whereas the stakeholders manage to obtain the source that documents the traced object [6].

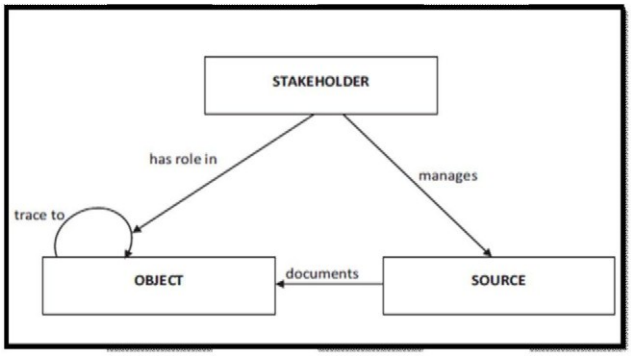

Fig1. Traceability Model [6]

Traceability model assists the investigator in identifying the relationship between the original sources of the evidence and the digital evidence along with the all the individuals involved in the digital investigation process. Plus, provides a precise and complete evidence of the case incident [6].

VIII. THE ENHANCEMENT OF THE TRACEABILITY MODEL BASED-ON SCENARIO FOR DIGITAL FORENSIC INVESTIGATION PROCESS

Traceability Model consists of 3 phases which are stakeholders, object and source. The three phases are connected and contributed to each other in finding the evidence and the relationship between the evidences found. As a result, we added the scenario phase in the top of the model which considers the first phase to have the initial planning of who will be the stakeholder and what are the objects and the sources needed to be found based on the scenario reported.

In [6] they have used scenarios at various stages of the development life cycle that describes the traceability requirements. Thus, it is important to have the scenario as the first phase in the model to have a clear understanding of the requirements and the related components of the traceability model. Moreover, this model is undefined in terms of the usage whereby the model only shows the three components of the traceability model and the relationships between each other. However, scenario describes the intended use or purpose of the model [6]. The Oxford English Dictionary definition of scenario is the script or the outline of a film, with details of an imagined sequence of future events or with a detailed of scenes [12].

Furthermore, scenarios have been a part of the models that represents a single or example of the sequence of the event [10]. Scenario is the field from the real world stories and description of requirements or models. Therefore, scenarios consider as examples of real world description of experience that is expressed in many forms such as picture, natural language or other media [13, 14].

Similarly, in requirement engineering scenarios can assist in testing the requirement specifications and the models during verification and validation of the requirement. Nonetheless, the advantage of using scenarios is when needed to have a supporting ground argument and reasoning with specific details [9]. Scenarios can help in creating a model, by looking for patterns of the details in the real world which gathers stories and description from users [12].

To expand on that, there are two requirement engineering methods that uses scenarios as one of the phases of the method, which are the ScenIC method and SCRAM, while many other requirement engineering methods uses scenarios as one of the elements of the method [12]. Additionally, the scenario phase is used to trace such any existing system behavior. Thus, scenario is understood by all stakeholders in requirements engineering [15].

Substantially, there are some methods such as Inquiry Cycle of Potts that used scenario to identify the problems and issues in requirement analysis [16] [17]. In fact, a scenario involved in the design phase and at many level of specific details. Though, some researchers have worked on identifying trace dependencies using scenarios [18]. But, some others also concerned to the tasks users can carry out in the design process, without involving in the lower-level details that describes how the system will use the functionality for the tasks to be carried out by the users [19][20].

IX. TRACEABILITY MODEL 0.2

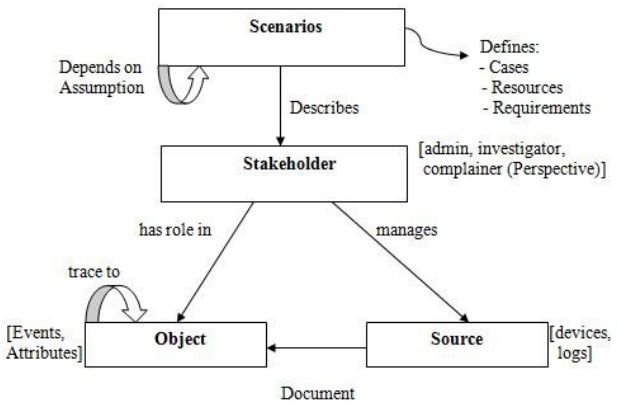

Fig2. Traceability Model 0.2

Traceability Model 0.2 is the second version of the first traceability model of digital forensic investigation process. It differs from the previous version that it has the Scenario as the first phase. Whereby, scenarios define the event cases, the needed resources, requirements and tools necessary to start the investigation and to have a clear idea of who will be the stakeholders as well as objects and the sources. The scenarios could be any case that must find its original traces such as, digital crime cases or system failure. Subsequently, scenarios describe the stakeholder that can be the admin, forensics investigator or complainer. Then, the stakeholders determine the object to trace events and attributes with managing the devices and the logs.

X. CONCLUSION

In this paper, we have reviewed the traceability models and discussed about the enhancement of the input process of the traceability model based on scenario in digital forensic investigation. Therefore, we can say that the traceability model 0.2 simplifies the process of tracing the source of the incident to the investigators of digital forensic investigation. The achievement gained in this research paper can be further improved by expanding the knowledge of the model to enhance some elements in the model as well as proving and specifying the forensic tools that can be used in the majority of the scenarios.

ACKNOWLEDGMENT

This work is a part of a research that has been done in Advanced Informatics School, under support from Universiti Teknologi Malaysia.

REFERENCES

[1] RSA 2012 cybercrime trends report http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf

[2] Bui, S., Enyeart, M., and Luong, J. Issues in Computer Forensics. *Santa Clara University Computer Engineering*, USA, 2003.

[3] National Institute of Standards and Technology (NIST), and United States of America. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. 2004.

[4] Siti, R. S., Shahrin, S., Nor, H., Robiah, Y., and Mohd, F. A. A Forensic Traceability Index in Digital Forensic Investigation. *Journal of Information Security*, (4) 19-32; 2013.

[5] Gary L Palmer. (2001). A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

[6] Selamat, S. R., Yusof, R., Sahib, S., Roslan, I., Abdollah, M. F., and Mas' ud, M. Z. Adapting Traceability in Digital Forensic Investigation Process. Malaysian Technical Universities

International Conference on Engineering & Technology (MUiCET 2011), 2-3; 2011.

[7] Katta, Vikash, and T. Stalhane. A conceptual model of traceability for safety systems. CSDM-Poster Presentation. 2010.

[8] Cleland-Huang, J., Hayes, J. H., and Domel, J. M. Model-based traceability. In Proceedings of the 2009 ICSE Workshop on Traceability in Emerging Forms of Software Engineering. 6-10; 2009. IEEE Computer Society.

[9] Wang, S., Shi, J., Jiang, D., and Qi, Z. Research for Traceability Model of Material Supply Quality in Construction Project. In Computational Intelligence and Design (ISCID), 2012 Fifth International Symposium on Vol. 2, 398-401; 2012. IEEE.

[10] Feng, Y., Huang, G., Yang, J., and Mei, H. Traceability between software architecture models. In Computer Software and Applications Conference, 2006. COMPSAC'06. 30th Annual International, Vol. 2, 41-44; 2006. IEEE.

[11] Dubois, H., Peraldi-Frati, M., and Lakhal, F. A model for requirements traceability in a heterogeneous model-based design process: Application to automotive embedded systems. In Engineering of Complex Computer Systems (ICECCS), 2010 15th IEEE International Conference on 233-242; 2010. IEEE.

[12] Sutcliffe, A. Scenario-based requirements engineering. In Requirements engineering conference, 2003. Proceedings. 11th IEEE international. 320-329; 2003. IEEE.

[13] Antón, A. I., and Potts, C. The Use of Goals to Surface Requirements for Evolving Systems. 1998 International Conference on Software Engineering: Forging New Links, on IEEE Computer Society Press. 157-166; 1998.

[14] Gough, P. A., Fodemski, F. T., Higgins, S. A., and Ray, S. J. Scenarios-an industrial case study and hypermedia enhancements. In Requirements Engineering, 1995. Proceedings of the Second IEEE International Symposium on IEEE. 10 -17; 1995.

[15] Carroll, J. M. Making use: scenario-based design of human-computer interactions. The MIT press. 2000.

[16] Alexander, I., and Maiden, N. (Eds.). Scenarios, Stories, Use Cases. John Wiley, 2004.

[17] Potts, C., Takahashi, K., and Anton, A. I. Inquiry-based requirements analysis. Software, IEEE, 11(2), 21-32; 1994.

[18] Sutcliffe, A. G., Maiden, N. A., Minocha, S., and Manuel, D. Supporting scenario-based requirements engineering. Software Engineering, IEEE Transactions on, 24(12); 1998. 1072-1088.

[19] Carroll, J. M. Scenario-based design. International Encyclopedia of Ergonomics and Human Factors, -3 Volume Set, 198. 2010.

[20] Egyed, A., A Scenario-Driven Approach to Traceability, Proceedings of the 23rd International Conference on Software Engineering (ICSE), Toronto, Canada, IEEE Computer Society, 123-132; 2001.