Adapting Traceability in Digital Forensic Investigation Process

Siti Rahayu Selamat, Robiah Yusof, Shahrin Sahib, Irda Roslan,
Mohd Faizal Abdollah, Zaki Mas'ud
Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka,
Durian Tunggal, Melaka, Malaysia

sitirahayu@utem.edu.my, robiah@utem.edu.my, shahrinsahib@utem.edu.my, irda@utem.edu.my,
faizalabdollah@utem.edu.my, zakimasud@utem.edu.my

Abstract

Generally, the goals of digital forensic investigation process in a cyber crime are to identify the origin of the incident reported as well as maintaining the chain of custody so that the legal process can take its option. However, the traceability process has become a key or an important element of the digital investigation process, as it is capable to map the events of an incident from different sources in obtaining evidence of an incident to be used for other auxiliary investigation aspects. Hence, this paper introduces the adaptability of the traceability model to illustrate the relationship in the digital forensic investigation process by integrating the traceability features. The objective of this integration is to provide the capability of trace and map the evidence to the sources and shows the link between the evidence, the entities and the sources involved in the process. Additionally, the proposed model is expected to help the forensic investigator in obtaining accurate and complete evidence that can be further used in a court of law.

Keywords: digital forensic investigation, traceability model, evidence, source of evidence

1. INTRODUCTION

Cyber crimes or digital crime are now serious, widespread, aggressive, growing, and increasingly sophisticated, which poses major implications for national and economic security [1]. Many industries and institutions, public- and private-sector organizations (particularly those within the critical infrastructure) are at significant risk. This statement has been proved by the number of complaints received and processed by the Federal Bureau of Investigation (FBI) in collaboration with Internet Crime Complain Center (IC3). In 2006, 200,481 complaints were received and has been increased in 2010 [2] as illustrated in Fig. 1.

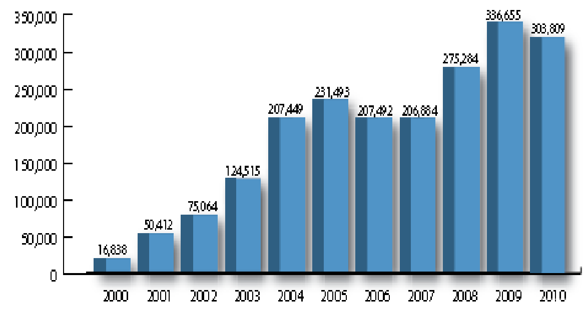

Fig. 1 Yearly Comparisons of Complaints Received Via the IC3 Website

This was a 34.01% increase as compared to 2010 when 303,809 complaints were received. From all complaints received in 2006 and 2010, IC3 referred 86,729 complaints and 121,710 complaints respectively to federal, states and local law enforcement agencies all around the country for further considerations. Although IC3 primarily refers complaints with claims of dollar losses, the top ten referred complaints indicate that 2.8% of complaints are computer intrusion and being increased to 9.1% in 2010.

From the cyber crime or complaints reported, it indicates that the number of crimes involving computers and internet has grown over the last decades and it needs products that can assist law enforcement in using computer-based evidence to determine the who, what, where, when, and how for crimes. As a result, computer and network forensics has evolved to assure proper presentation of computer crime evidentiary data into court and the role of forensic become highly important to get digital evidence.

The purpose of a forensic investigation can be established by either identifying the offender of a case, or establishing an evidence to build a case against the offender [3]. As both situations are common in the law enforcement perspective, the ability to trace the source to an evidence or vice versa is essential [4]. Additionally, another limitation is the acceptability of evidence that differs in each of these situations. There was also an issue of origin identification and cross referencing in investigation process [5] [6]. Hence, the traceability information is important to avoid the mislaid of decision and valuable information in collecting and analyzing during the investigation process.

Due to this fact, the goal of this research is to adapt and integrate traceability in the digital forensic investigation process that represents the traceability information in the stage of conceptual and component composition. The purpose of this integration is to help the forensic investigator obtain accurate and complete evidence of the incident. In this paper, the proposed adaptation will be constructed based on the malware intrusion scenario.

The rest of the paper is organised as follows: The next section explains the related work on traceability, traceability models and digital forensic investigation process. Section III further describes the integration traceability in digital forensic investigation. The adaptation of traceability model is proposed in Section IV and a conclusion, together with future works is summarized in the last section.

2. RELATED WORK

2.1 Overview of Traceability

Traceability is the means to identify and follow real or imaginary objects through a process chain [7]. It gives the opportunity to back-track a chain of events, or to predict process outcomes given in the origin of an object. Traceability can be used in different areas. Even though traceability can also be defined in many ways, the meaning is to be able to trace and get information. ISO 8402:1995 defines traceability as the ability to trace the history, application or location of an entity, by means of recorded identifications.

Traceability is a tool to achieve different objectives and can never be completed. Therefore, [8] described the definition of traceability can be broad, because in most of the time the processes are very complex. On the other hand, [9] defined traceability as the ability to map events in cyberspace, particularly on the Internet, back to real-world instigators, often with a view to holding them accountable for their actions. In contrast, [10] define traceability in the networks perspective as how difficult it is to establish the source and destination of communications on computers and communication networks, such as the Internet. Therefore, based on the definition reviewed in this research, this paper summarized the definition of traceability as the ability to trace and map the events of an incident from difference sources in order to obtain evidence of an incident for further process of investigation.

In order to trace the requirement, the traceability approach is needed. Hence, [11] suggested that tracing the requirement can be performed in several ways based on the direction of tracing activities that are forward traceability and backward traceability as depicted in Fig.2.

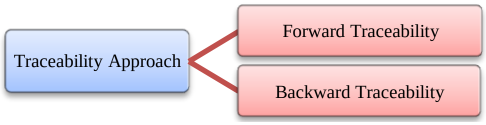

Fig. 2 Basic Traceability Approach

Forward traceability approach defined in [12] is the ability to trace a requirement to components such as a design or implementation whereas backward traceability is the ability to trace requirement to its sources such as a person, institution, and argument. This basic concept of these traceability approaches can be represented as in Fig. 3.

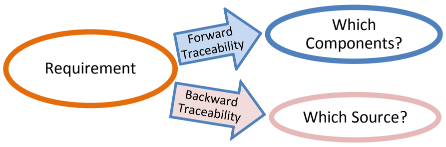

Fig. 3 Concept of Backward and Forward Traceability

Forward traceability approach is common in software requirements perspective. In this approach, all related test procedures used to ensure the test procedures comply with the changed requirement and the components built to meet the requirement can be obtained. Thus, it is used to investigate the impact of the requirement's change [11] [13] in which it provides the ability to analyze the changes on the components.

Meanwhile, backward traceability approach is used when the stakeholder is required to understand the changes happen such as when, what and how the requirement changed by investigating the information used to describe the changed requirement. In this approach, several useful information that point towards to the source will be obtained such as who the person interested in the requirement is, what documents from which requirement was extracted are, which departments the requirement is related, and when the changes to the requirement is done.

However, [13] [14] [15] suggested that in order to have a well managed requirements, traceability can be established from the source requirements to its lower level requirements and from the lower level requirements back to their source. This reveals that it is necessary to trace a requirement to the artifacts that implement it as well as tracing from an artifact to the requirement that the artifact itself implements. This circumstances create an idea on tracing in both ways, forward and backward or called as bidirectional approach as discussed in [16]. Hence in order to provide an accurate and complete evidence to prosecute the offender, this research will use the traceability approach discussed in [16]. To demonstrate the approach, knowledge of organizing the procedures, techniques and tools are needed. Identified as a traceability model, this knowledge is discussed in the next sub-section.

2.2 Traceability Model

A traceability model is a central component of a traceability environment around where the tracing procedures, techniques or methods, and tools are organized. A traceability model not only defines what entities and traces are, and which traces should be captured, but also represents traceability information in the stage of conceptual design, component composition, deployment and runtime [17] [18] . However, based on [18] [17] [11], the traceability model is used to represent the traceability information which demonstrate the relationship between the traces, entities and sources involved in a process or system.

In a traceability model, the conceptual explanation is covered by three features, namely the definition, the production and the extraction of traces [11]. The definition feature is concerned with the specification of the traces and traceable objects. It is within this feature that traceability model should define its traces, attributes and represented method. The definition of traces and traceable objects should promote a uniform understanding in order to avoid any errors caused by different interpretation during the tracing activities.

The production feature is concerned with the capture of traces that is usually by the means of an explicit registration of the objects and their relationships. The trace production deals with the actual occurrence of traces that roughly corresponds to the pragmatics of a traceability model in order to get a constructive traceability model.

The extraction feature of the traceability model is concerned with the actual process of tracing such as the retrieval of registered traces. A traceability model should provide diverse and flexible ways to retrieve (extract) the information registered in it as discussed in [19].

Consequently, a traceability model should provide a representation for traces and trace attributes as discussed in [17] in which the trace model provide two significants guidelines; relationship guideline and tracing guideline. The former guideline describes the relationship guidelines that explain what traces should be established and the later guideline describes how traces determined by the relationship guidelines should be documented. Both guidelines establish the structures containing the elements and the relations used in tracing, specifying their type as well as the constraints under which elements of the model can be related.

Hence, this research will employ all three features of the traceability model by adapting and integrating the features into the forensic investigation process. The goal of this adaptation and integration is to acquire accurate and complete evidence traces to help the forensic investigator on investigation process especially on collecting the evidence and the evidence sources of an incident.

2.3 Digital Forensic Investigation Process

In the digital forensics investigation practices, there are over hundreds of digital forensics investigation procedures developed all over the world. Each organization tends to develop its own procedures and some focused on the technology aspects such as data acquisition or data analysis [20]. Most of these procedures were developed for tackling different technology used in the inspected device. As a result, when underlying technology of the target device changes, new procedures have to be developed.

A research done in [21] introduced a mapping process which occurs inside digital forensic investigation process model. The mapping is formulated by grouping and merging the same activities or processes in five phases that provide the same output into an appropriate phase. From the analysis, most of the models consist of the critical phases which are Phase 2 – Collection and Preservation, Phase 3 – Examination and Analysis, and Phase 4 – Presentation and Reporting except Phase 1 and Phase 5. Even though, Phase 1 and Phase 5 are not included in some of the model reviewed, the study done by [22] [23] [24] [25] [26] [27] [28] [29] [30] indicate that both phases are important to ensure the completeness of the investigation. Phases 1 is to ensure the investigation process can start and run in the proper procedure, and protect the chain of evidence. While by eliminating Phase 5, it will lead to the possibility of the incomplete investigation and no improvement in investigation procedures or policies. Therefore, a good model should consist of all important phases; Preparation Phase, Collection and Preservation Phase, Examination and Analysis Phase, Presentation and Reporting, and Disseminating the case.

[21] findings also show that the existing models mentioned in each of the proposed models build on the

experience of the previous; and some of the models have similar approaches and some of the models focus on different areas of the investigation. However, all of the models in the output mapping have the same output even though the activity is slightly difference on the term used and the order of the steps. On the other hand, all of these frameworks identified in the output mapping show that each framework has their own strength; however until nowadays there is no single framework that can be used as a general guideline for investigating all incident cases.

Therefore, in order to obtain the evidence and for it to be accepted in the court of law, digital forensic investigation must be successfully performed without tampering the evidence. Additionally, the chain of evidence should be presented to prove the evidence is legitimate. Hence, the evidence traceability identification of the origin of the crime scene or the location of the incident or crime originated is one of the important elements during the digital forensic investigation process and become the first challenge in the investigation as mentioned in [6] [31] [32].

3. TRACEABILITY IN DIGITAL FORENSIC INVESTIGATION PROCESS

In digital forensic investigation process, tracing is described as a process of finding or discovering the origin or cause of certain scenario. The tracing activities are able to discover the traces left in digital devices. In the computer crime perspective, trace can be found in any digital devices. These traces consist of activities such as login and logout of the system, visit of pages, accesses documents, create items and affiliation groups found in records of data. These traces data are analysed by identifying their relationship among the attributes such as port, action, protocol, source IP address and destination IP address where this consistent relationship will produce trace pattern of the incident or crime. This trace pattern can be further used on assisting the investigator during the investigation process.

3.1 Incident Trace Pattern

Incident trace pattern is essential in assisting the investigators tracing out the evidence found at crime scenes [33]. In this research, we affirm the definition of trace as any digital evidence in an incident. Meanwhile, tracing is defined as the observation of the moving trace on the various tracks. In addition, pattern is defined as a regular way in which certain scenario happened [34]. Therefore, in order to get a trace pattern, the observed movement of these trace is studied to confirm its regular way, with the help of the acquired hypothesis.

The incident trace pattern is confirmed using two steps. Firstly, the hypothesis which explains the initial scenario of the incident is taken. Secondly, the trace which was recorded in the source of evidence (host and network logs) is formulated. Using these two, the movement is observed which conclude that within the source of evidence, there are three courses of action that occurred. This course of action is referred as an *event* instead of process due to their focuses. A process merely focuses on progress or series of action toward a particular result; whereas, an event focus on the occurrence of something which not only concern with its action, but also with the attributes associated with it [35].

The extraction of the two steps above derives the three events of incident which are *scan*, *exploit* and *impact/effect*. *Scan* consists of the inspection activity which are not only to find vulnerability, but also to determine any available services (e.g. port number) on the target system (system being attacked) [36]. In this activity, if the port number responds to a scan, it will indicate the type of service running on the target system and reveal the exploitable services to attackers. Therefore, once the system determined which services are running on it, the vulnerability of the system could be exploited. Eventually, these exploited vulnerability can become a threat, such as unauthorized access (gain access) or unavailable service for intended users (deny service).

Exploit consists of the abuse activity traces that disclose any manipulation activity on the target system services such as attempting on downloading malicious codes to the target system and breaking the target system for opening backdoor on specific port. Meanwhile, the *impact/effect* event shows the traces on the goal of an attack which shows the goal of an attack as the consequences of the scan and exploits activities of the incident such as the target system is restarted, the services are terminated (expectedly) and new process is forced to be created.

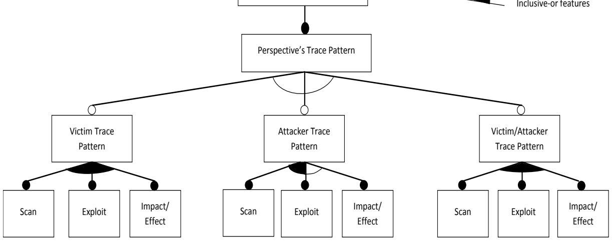

Fig. 4 Event-based Forensic Trace Map

In this research, the combination of the three events discussed previously form different trace patterns in order to identify the offender of the incident: victim, attacker and victim/attacker. As this pattern reflects the complainer or perspective, henceforth, it is named as *Perspective Trace Pattern*. From the analysis and findings in [33], victim/attacker and victim perspective trace pattern must consists of all three events, and attacker perspective trace pattern must consist of *scan* and *exploit* events of incident but it is optional in having the *impact/effect* event as depicted in Fig. 4. However, the difference between them is the content of the attributes belongs to each of the events such as the number of the destination port open, the type of operation, the protocol of the connection request, the services that are vulnerable and the item transferred during the communication exist.

The attributes of *scan* are *communication exist*, *destination port open*, *operation type* and *connection request*. Conversely, the attributes of *exploit* event are similar to *scan* event, with an addition of *vulnerable service* attribute. Nevertheless, the attributes of *impact/effect* are *communication exists*, *new process creates*, *malicious code transferred* as well as *service terminated*.

For the purpose of this paper, in explaining perspective trace pattern, let's consider an incident that was caused by a worm, Sasser. Based on the logs (host and networks), the traces of *scan* event shows the attribute of *communication exist* between the victim and attacker via *Destination IP Address* and *Source IP Address* respectively. Next, the destination port open responded is port *445* and the operation type (action) is *OPEN* (in/out communication is allowed), whereas the connection request (protocol) is *TCP* (traffic packet is transmitted). The success of this event leads to the next event, *exploit*. In this event, the action continues with destination port open responded is *9996* and *5554*. If the port *9996* is exploited, the operation type (action) is *OPEN* and the connection request is *TCP*, then partial exploit is in place. Port *5554* is also exploitable. If port *5554* is exploited, the operation type (action) is *OPEN-INBOUND* (traffic is allowed in) and the connection request is *TCP* (file is transmitted) which leads to vulnerable service (service) as *FTP* (file transfer occurred). We consider the exploit is successful if both ports above are exploited. As the consequences of the scan and exploit event, the *impact/effect* incident occurred. This event consists of few attributes namely; a) *offender identified* (who is victim and attacker), b) a process created (traffic action) which reside at *%WINDIR%\System32\ftp.exe*, c) the *service terminated* is *lsass*, and d) *malicious code transferred* (file transmitted) is *~*.exe*. The above example describes that the traces belong to attacker trace pattern. The example can also be represented as an algorithm depicted in Table 1.

Table 1 Attacker Trace Pattern Algorithm

Attacker Trace Pattern

```
Event Name: Scan
Attribute:-
    Communication Exist   := Source IP Address,
                             Destination IP Address
    Destination Port Open := 445
    Operation Type        := OPEN
    Connection Request    := TCP
Action  :- find_vulnerability( );
           determine_services( );
```

```
Event Name: Exploit
Attribute:-
     Communication Exist   := Source IP Address,
                              Destination IP Address
     Destination Port Open := 9996 || 5554
     Operation Type        := OPEN || OPEN-INBOUND
     Connection Request    := TCP || TCP
     Vulnerable Services   := FTP (9996 && 5554)
Action  :- scan( );
           show_manipulation_activity( );
```

```
Event Name: Impact/effect
Attribute:-
    Offender Identified          := Attacker
    New Process Created          := %WINDIR%\System32\ftp.exe
    Malicious Codes Transferred := ~\*.exe
    Service Terminated           := lsass
Action  :- exploit( );
           show_impact( );
```

3.2 Integration of Traceability Features and Digital Forensic Investigation Process

In order to provide the capability of tracing and mapping the accurate and complete evidence in digital forensic investigation process, the relationship between each trace should be identified to form the incident trace pattern. In this research, the ways for identifying this relationship is accomplished using features in traceability approach (definition, production and extraction) discussed previously. The integration of the traceability model's features (TMF) in digital forensic investigation process (DFIP) is illustrated in Table 2.

In Table 2, TMF in DFIP indicate that there is a potential in implementing traceability features in forensic investigation process. As mentioned by [6] [37], traceability is an important element in forensic investigation process and it is related to the link element which is the key element used to form evidence's chain of custody. It is impossible to prevent all internet misuse but it is not impossible to identify and trace the evidence, and then take appropriate action.

Table 2 The Integration of TMF and DFIP

Feature	TMF	TMF in DFIP
Definition: related to the specification of the traces and traceable objects	identify traces, attributes	identify component in incident
Production: related to the capture of traces (relationships)	perception, registration and maintenance	hypothesis, identify forward and backward traceability, preservation of evidence
Extraction: related to the actual process of tracing	trace extraction mechanism	tracing the evidence using selective tracing to promote trace pattern

Therefore, without the traceability information, the investigation decisions and other valuable information for collecting and analysing the evidence could be mislaid. Hence, a traceability approach is necessary and in this research, the proposed integration is named as trace map model.

3.3 Proposed Adaptation of Traceability Model in Digital Forensic Investigation Process Model

The proposed adaptation of traceability model in digital forensic investigation process model is based on work done in [33] and later known as *Trace Map Model*. This model uses event-based traceability technique which was motivated from the traceability model discussed in [38]. Ramesh introduced three components: *stakeholder*, *subject* and *object*.

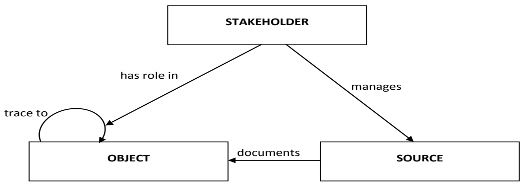

Fig. 5 Traceability Model [38]

In this model, the *stakeholder* represents people who have an interest on requirements and on the tracing of requirements, the *source* represents the origins of a requirement and the artifacts used for documentation purposes, and the *object* represents the inputs and outputs being traced. In Fig. 5, the model represents what type of information is presented including salient attributes or characteristics of the information which is referred as *object*. For example, this information can be represented as an attribute of *object* and the traceability across various *object* is represented by a link namely *traces to*. The model also shows the *stakeholders* are the people who play different roles in the creation, maintenance and use the various *objects* and traceability links across them. These *stakeholders* act in different roles or capacities in the establishment and use the various conceptual *object* and traceability links. The *subject* represents the location of the documented traceability information i.e. which state that all objects are documented by subjects.

Various dimension of traceability information is discussed in Ramesh's model such as what kind of information is represented, who are the people that play the role, where and how the traceability information are represented, why and where the object are created, modified and evolved. The compatibility and the capability model also have been discussed in various business areas with different traceability focus. In this research, this model is adapted and integrated within the digital forensic investigation process which consists of three components, namely *stakeholder*, *source of evidence* and *digital evidence* as shown in Fig. 6.

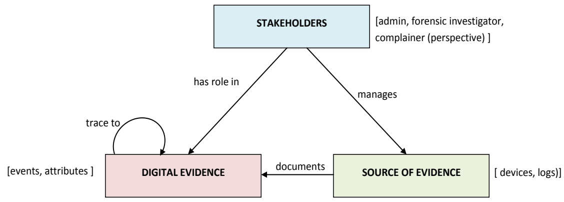

Fig 6 Conceptual Diagram of Digital Forensic Investigation Process

These components map to the components in Ramesh's model: *stakeholder*, *subject* and *object* respectively. *Stakeholders* refer to the people involve in the whole process of digital forensic investigation such as the auditor, network administrator, complainer (perspective as discussed in [33]) and forensic expert. In this research, these investigators will manage the *source of evidence* on the incident reported such as the devices (host and network) and the logs involved in the incident. Meanwhile, the *digital evidence* is defined as events of incident (see subsection Trace Pattern) that are documented in the source of evidence. This current relationship is further depicted using the diagram in Fig. 7. For the purpose of this research, the domain selected is malware intrusion incident.

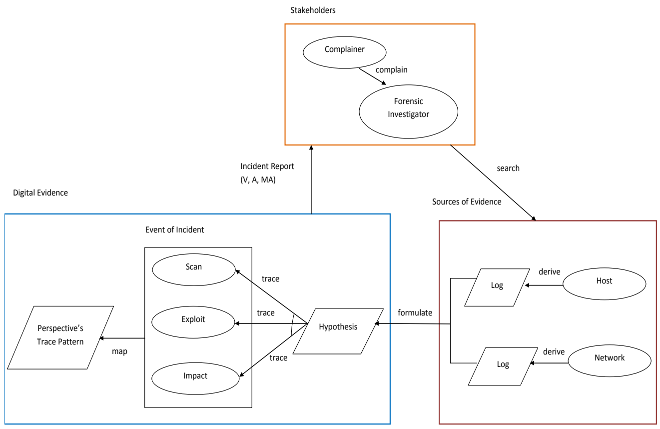

Fig.7 Trace Map Model

Fig. 7 depicts the process of investigation is initializes when a complainer complains or reports the incident to the investigator (administrator and/or forensic investigator). Then, the process is continued by searching the relevance potential evidence based on the preliminary information reported by the complainer. The evidence is collected from the source of evidence: host and network that derive heterogenous log. Subsequently, a hypothesis (an assumption made to test the logical or empirical consequences) is formulated in order to trace the event of the incident. The traces of event gathered then are map to construct the perspective's trace pattern.

Based on the proposed *Trace Map Model*, the investigator could trace and map the traces of the incident that are used as the digital evidence of the incident. In this model, the traces of the offender are based on the primary events of incident that *scan*, *exploit* and *impact/effect*. In each event of incident, the trace patterns of the perspectives (victim, attacker, multi-step attacker) are established. The model also assists the investigator on identifying the relationship between the source of evidence, the digital evidence and the people involve during the investigation process, and provide a complete and accurate digital evidence of the incident reported.

4. CONCLUSIONS AND FUTURE WORKS

Traceability is an important element in forensic investigation process and related to the link element which is the key element used in forming the chain of evidence. Therefore, this research introduced a *Trace Map Model* that derived from the adaptation and integration of the traceability in digital forensic investigation process. The proposed model is used to provide the forensic investigation the capability to trace and map the digital evidence and source of evidence during the forensic investigation process.

This capability of the model is based on the preliminary assessment through the case study as presented in this paper. It also shows that the trace pattern enables us to identify the origin of malware intrusion through the traces attributes. These assist the investigator to show the relationship of the incident traces for obtaining the evidence accuracy and completeness that could enable the legal process to take its due course. In future, the effectiveness of the evidence tracing and mapping is evaluated through a validation process. It is foreseeable to develop a prototype that can be used as one of the forensic investigation tool through this proposed model.

ACKNOWLEDGMENT

We thank Universiti Teknikal Malaysia Melaka for the Short Grant Funding for this research project.

REFERENCES

[1] Deloitte, *Cyber Crime: A Clear and Present Danger; Combating the Fastest Growing Cyber Security Threat*. 2010, Center for Security & Privacy Solutions. p. 1-16.

[2] IC3, *2010 Internet Crime Report*. 2011, National White Collar Crime Center (NW3C). p. 24.

[3] Jansen, W. and R. Ayers, *Guideline on Cell Phone Forensics*, in *NIST Special Publication 800-101*. 2007, National Institute of Standards and Technology: Gaithersburg.

[4] Rogers, M.R., *The role of criminal profiling in the computer forensics process.* Computers & Security, 2003. **22**(4): p. 292--298.

[5] Casey, E., *Digital Evidence and Computer Crime*. Second ed. 2004: Elsevier Academic Press.

[6] Stephenson, P., *A Comprehensive Approach to Digital Incident Investigation*, in *Elsevier Information Security Technical Report*. 2003, Elsevier Advanced Technology.

[7] Oghazi, P., B. Pålsson, and K. Tano. *An attempt to apply traceability to grinding circuits*. in *Conference in Mineral Processing*. 2007. Luleå, Sweden.

[8] Golan, E., et al., *Traceability in the U.S. Food Supply: Economic Theory and Industry Studies*, in *Agricultural Economic Report* 2004.

[9] Clayton, R., *Anonymity and Traceability in Cyberspace.*, in *Computer Laboratory, Darwin College*. 2005, University of Cambridge. p. 189.

[10] Lázaro, P.G.-C., *Forensic Computing from a Computer Security Perspective*, in *Information Theory*. 2004, Linköping Institute of Technology. p. 143.

[11] Pinheiro, F.A.C., *Requirements Traceability* in *Perspectives on Software Requirements*. 2004, Kluwer Academic Publishers: Netherlands. p. 91-113.

[12] Wieringa, R.J., *An Introduction to Requirements Traceability* 1995, Faculty of Mathematics and Computer Science, University of Vrije Amsterdam.

[13] Morckos, M., *Requirements Traceability*. 2011, University of Waterloo. p. 4-5.

[14] Zemont, G., *Towards Value-Based Requirements Traceability*, in *Department of Computer Science*. 2005, DePaul University: Chicago Illinois.

[15] Narmanli, M., *A Business Rule Approach to Requirements Traceability*. 2010, Middle East Technical University. p. 8-9.

[16] Westfall, L., *Bidirectional Requirements Traceability*. 2006.

[17] Knethen, A.V. and M. Grund. *QuaTrace: A Tool Environment for (Semi-) Automatic Impact Analysis Based on Traces*. in *IEEE International Conference on Software Maintenance (ICSM'03)*. 2003. Amsterdam, The Netherlands.

[18] Feng, Y., et al. *Traceability between Software Architecture Models*. in *Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC'06)*. 2006: IEEE Computer Society.

[19] Pinheiro, F.A.C. and J.A. Goguent, *An Object-Oriented Tool for Tracing Requirements.* IEEE Software, 1996. **13**(2): p. 52-64.

[20] Brill, A. and M. Pollitt, *The evolution of computer forensic best practices: an update on programs and publications.* Journal of Digital Forensic Practice, 2006. **1**: p. 3-11.

[21] Siti Rahayu, S., Y. Robiah, and S. Shahrin, *Mapping Process of Digital Forensic Investigation Framework.* International Journal of Computer Science and Network Security, 2008. **8**(10): p. 163-169.

[22] Baryamureeba, V. and F. Tushabe. *The Enhanced Digital Investigation Process Model*. in *Proceeding of Digital Forensic Research Workshop*. 2004. Baltimore.

[23] Carrier, B. and E. Spafford, *Getting Physical with the Digital Investigation Process.* International Journal of Digital Evidence, 2003. **2**(2).

[24] Ciardhuáin, S.Ó., *An Extended Model of Cybercrime Investigations.* International Journal of Digital Evidence, 2004. **3**(1).

[25] Roger, M., *DCSA:Applied Digital Crime Scene Analysis*. 2006: Tipton & Krause.

[26] Reith, M., C. Carr, and G. Gunsch, *An Examination of Digital Forensic Models.* International Journal Digital Evidence 2002. **1**(3).

[27] Beebe, N.L. and J.G. Clark. *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process*. in *Digital Forensic Research Workshop*. 2004. Baltimore.

[28] Freiling, F.C. and B. Schwittay. *A Common Process Model for Incident Response and Computer Forensics*. in *Proceedings of Conference on IT Incident Management and IT Forensics*. 2007. Germany.

[29] Kohn, M., J. Eloff, and M. Olivier. *Framework for a Digital Forenisc Investigation*. in *Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference*. 2006. South Afrika.

[30] Perumal, S., *Digital Forensic Model Based on Malaysian Investigation Process.* International Journal of Computer Science and Network Security, 2009. **9**(8): p. 38-44.

[31] Casey, E. and G.L. Palmer, *The Investigative Process*, in *Digital Evidence and Computer crime*. 2004, Elsevier Ltd.

[32] Stephenson, P., *Getting The Whole Picture Volume 1*, in *End-to-End Digital Investigation*. 2003, Getting The Whole Picture Volume 1. p. 19-20.

[33] Siti Rahayu, S., et al., *Advanced Trace Pattern For Computer Intrusion Discovery*. Journal of Computing, 2010. **2**(6): p. 1-8.

[34] Fernandez, E., J. Pelaez, and M. Larrondo-Petrie, *Attack Patterns: A New Forensic and Design Tool.* IFIP International Federation for Information Processing, 2007. **242**: p. 345-357.

[35] Carrier, B. and E. Spafford. *An Event-based Digital Forensic Investigation Framework*. in *Digital Forensics Research Workshop*. 2004. Baltimore, MD.

[36] Liu, Z., C. Wang, and S. Chen, *Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern Modeling.* IEEE Computer Society, 2008: p. 214-219.

[37] Palmer, G., *A Road Map for Digital Forensic Research*. 2001, Digital Forensic Research Workshop (DFRWS): Utica, New York.

[38] Ramesh, B. and M. Jarke, *Towards Reference Models For Requirements Traceability.* IEEE Transactions on Software Engineering, 2001. **27**(1): p. 58-93.