International Conference on Computational Science and Information Management (ICoCSIM)
Vol. 1 (2012) 251-258

A Defensive Evidence Model: An Approach of Security Model for Storing Digital Evidence in Network Forensics

Mohd Izham Ibrahim[a], Aman Jantan[b], Mohammad Rasmi[b]

[a]Faculty of Computer System and Software Engineering, Universiti Malaysia Pahang, 26300, Pahang, Malaysia
[b]School of Computer Science,Universiti Sains Malaysia,11800, Pulau Pinang, Malaysia

mohdizham@ump.edu.my, aman@cs.usm.my, mr77mr@hotmail.com

Abstract

Network Forensics Investigators apply most of the network monitoring tools, such as Snort or WinPcap to monitor or identify potential evidence to be collected and stored. However, these tools are lack of protection mechanisms to keep the evidence safe as well as the rising issues of chain-of-custody that are not properly managed or addressed. Therefore, people with intentions may disrupt the collection process and tampered the contents of the stored evidence. Considering these issues, this paper proposes a Defensive Evidence Model (DEM) to manage the evidence collection processes as well as providing defensive measures to protecting the evidence. Features of DEM were adapted from four security models; Bell-LaPadula, Biba, Clark-Wilson and Goguen-Meseguer Model and integrated with the Forensics Investigation process. The assessment of DEM performed from two different aspects, first by analyzing the attack and second, evaluating the process through CIAA security requirements to determine the workability of the created model.

Keywords-network forensics; evidence preservation; security model; security requirement process;

1. Introduction

According to Malaysian Computer Emergency Response Team (MyCert) in CyberSecurity Malaysia[1], there are 15,218 cyber incidents being reported in the fourth-quarter of 2011. The number of cases keep adding up as until February 2012 it increase with 954 cases being reported. Cases reported such as Intrusion Attempt, Denial of Service, Fraud, Vulnerability Report, Cyber Harassment, Content Related and Malicious Codes. The rise of cyber-crime incidents is a major threat against the nation and the possibility of capturing criminals in certain cases such as Intrusion or Denial of Service need a proper digital forensics investigations technique and tools to convict the criminals.

Since most of Intrusion or Denial of Services involve in networked environment, the use of Network Forensics investigations is important to analyze and gathering the evidence. Network Forensics derived from Digital Forensics with process of capturing, recording and analyzing network packets or events. The purpose of this process is to examine network packets for source of the problem and gather information about criminal or malicious activities[2]. However, the role of Network Forensics to conduct crime investigations only works best in a networked environment with networking tools being set up earlier to find anomalies. The use of network monitoring tools is crucial to detect and filter malicious activities from common activities that are running.Network monitoring tools such as Intrusion Detection System (IDS) was used to monitor and record data in transit in order to detect potential attacks[3]. A recent study in 2011 by Ahmad Qaisi shows that using IDS to find possible evidence was difficult for forensics investigations as the collected data was stored in log files or database with different forensics structure or file format[4]. Moreover, to analyze possible evidence or information related to the crime incident were done manually and consume lots of time and resource.

Other monitoring tools used for analyzing and detecting anomalies or possible evidence such as Snort or WinPcap were also not equipped with the mechanisms to protect and preserve the collected data. Although these tools were not built for preserving purpose, they do support the mechanisms to keep the integrity of the data and provide the hash value of the data for future reference. The technique is very practical in computer forensics investigations. However, if the data was tampered at the beginning of the process of collecting it, then the purpose of keeping safe the false evidence might not be very useful.In addition, these tools are also not able to detect who conducts the investigations or who collected the evidence or who is the last person to have accessed to the evidence. Thus, access control is not properly addressed in these tools and could lead to the problem of proving the chain-of-custody of the evidence. These issues should be solved by providing monitoring tools for network forensics which include mechanisms to protect the collected evidence and at the same time preserving the chain-of-custody of the evidence until it is presented in Courts of Law.It is the requirements of Courts that needs the procedure and technique chosen to be valid and admissible. According to Carrie in 2006, most of the corporations and intelligence agencies conducting investigations were not using proper methods to find evidence, which makes some of their results being rejected in Courts of Law[5]. Moreover, during analyzing the evidence, any modification should be recorded and reported so that there will be no issues of evidence tampering while doing investigations. However, the lack of formal training and knowledge among the investigators will worsen the problem and the process to apprehend the criminal in Courts of Law will be disturbed.

The objective of this paper is to provide a model for Network Forensics works with the enhancement of security for tools and procedure in preserving the collected evidence. Apart from that, the chain-of-custody of evidence will be managed and addressed properly. The mechanisms of the proposed Defensive Evidence Model were adapted from features of security models such as Bell-LaPadula, Biba, Clark-Wilson and Goguen-Meseguer Model. Each security feature is cross-linked with the phases of forensics work as proposed by S.R.Selamat. The process of linking the security model with the process identified by S.R.Selamat is needed as it suggests a standard forensic work[6]. Existing phase was concluded from various frameworks, and they share the common phase as shown in Table 1.

Table 1. Digital Forensics Investigations Phases [6]

Phase	Phase Name
1	Preparation
2	Collection and Preservation
3	Examination and Analysis
4	Presentation and Reporting
5	Disseminating the case

The goal of Network Forensics Investigation is to prepare, collect, preserve and examine data without compromising the integrity of the evidence. However, during the preservation of the evidence, the data are exposed to attack and tampering by various threats either by an inside or outside attacker. Through the identified problems from the forensics work and process, the security model analyzes the workability of DEM to be used in Network Forensics. Next section will explain the security models, and the security features to be link with forensics work in brief.

1.1. Security Model

Security model was defined as a formal description of security policy which is the steps to be taken to achieve secure environment or secure entity. According to Fisch and White, in order to develop a secure system, a formal model for the security should be included as part of the top-level definition of the system[9]. Selected types of model mentioned by Fisch and White are Bell-LaPadula Model, Biba Integrity Model, Clark-Wilson Integrity Model, and Goguen-Meseguer Model. The chosen model is based on the objective of a forensic system to achieve admissible forensic evidence that concentrates on producing high integrity

Bell-LaPadula Model – The Bell-LaPadula Model often resemble a state machine model that force access control and deals with the confidentiality issues of the protected data[9]. This model consists of a set of Subjects, a set of Objects, and an access control matrix. Each subject has a clearance, and each object has a classification which attaches it to a security level as shown in Figure 1. However, the subject clearance level will not exceed the upper clearance level and only allowed to change clearance level below its assigned clearance level. Furthermore, the access rights given to a subject are Read-Only that allowed file to be read without modifications, Append that allowed the file to be written new item, Execute that allowed file to running specific function and Read-Write which allowed file to be modified when read. However, according to Fisch and White, there are restrictions on Bell-Lapadula Model with no read up and no write down,and the model might still become too restrictive if the object's security level being static[9].

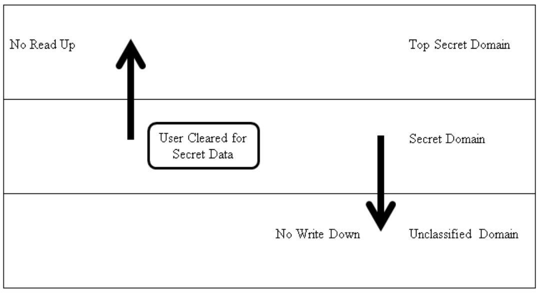


Figure 1. Bell LaPadula Model[9].

Biba Model – The Biba Model are more focus on the integrity of the computer system by delivering computer security policy that describes access control rules to address integrity in the computer system to prevents unauthorized users from making modifications[9]. Common area of use for this model is in military field where subjects may not corrupt objects in a level rank higher than the subject, or be corrupted by objects from a lower level than the subject. Recent work by Arthur in 2010 utilized Biba

Model to manage the integrity of data in the proposed Forensic Evidence Management system[10]. The model was used to categorize evidential data into integrity classes, where any application is only allowed to read evidence with a higher (or equal) integrity classification than its own. Different from Bell-LaPadula Model, this model focus on the integrity of the data and have restrictions of no read down and no write up.

Clark-Wilson Model – Different from Biba Model which focuses on military and government operation, this model has more priority in the commercial data processing environment as it is related to the integrity of data itself rather than confidentiality to users who access. The use of this model is controlled by program rather than directly accessing the data itself. Users who are accessing the program are assigned to different roles and need to collaborate to achieve secure operation. Most important about this model is that, it insists on the auditing the transaction and the flow of the system, which makes the process of detecting breaches easier.

Goguen-Meseguer Model – The Goguen-Meseguer Model introduces the concepts of non-interference between users and prohibited usersfrom high to lower level to interact. This restriction is based on the activities' similarity between the users if both issued same commands, then the outputs are also the same. The model is based on Multilevel secure and achieve non-interfering unless the first user have less or same level with the second user. The concepts of Goguen-Meseguer Model concentrate on the idea of separating users based on their protection domains and avoid access from the same domain.The issues of integrity and confidentiality of the evidence are important in the Defensive Evidence Model as the evidence stored can achieve protection and security. However, to design top level security on the system for monitoring and storing the evidence, the security feature of the system for forensics work should be considered.

1.2. Security Features for Protecting Evidence in Network Forensics

In cyber-crime investigations, evidence that are attacked or tampered with would raise lots of questions when presented in Courts of Law. The nature of the evidence collected from several places such as computer systems, networks, wireless communications and storage devices are very tangible and might be lost when transmitted. Thus, it is important to understand the types of evidence need to be collected so that specific measures were taken to handle and secure such evidence. There are three basic types of data collected during investigations; persistent data, volatile data and network data[7]. Our focus in this paper will be on network data that consists of information about the packets, the protocol, IP addresses, ports and number of packets.

Evidence that was collected in forensically manners are still open to debate in the Court of Law as tools used to collect the evidence more often than not, lackedthe security measure required to protect the evidence. The lack of technical understanding about the process of the computer and network environment would also lead to inadmissible evidence. A recent study by R.Hunt in 2010 address the importance of computer security and forensic analysis from a real-time perspective. The author had shown the possibility to monitor security events in a live network environment while conducting forensics work to collect, store and process the evidence. However, there is no security model being discussed to deliver reliable evidence, which makes the possibility of data tampering as a threat.

According to Krutz in 2003, security model was categorically based on four different modes. The mode of operation is determined by[8]:

- The type of users who have access to the system either directly or indirectly
- The type of data that are processed on the system.
- The type of levels of users, their need to know, and the formal access approvals.

As shown in Table 2, the difference in security mode is based on either all information or some information if 1) user sign Non-disclosure agreement, 2) user has proper clearance, 3) user has formal access approval, 3) user has a specific need to know or necessary for official duties. However, in a Digital Forensics Investigation, the process of collecting and storing the evidence requires more parameters to maintain the chain-of-evidence so that the evidence is accepted in a Court of Law, thus a dedicated security mode with more permission to access should provide more security in protecting the evidence.

Table 2. Security Mode Operation

Mode	Non-disclosure agreement	Proper Clearance	Formal Access Approval	Need to know
Dedicated Security Mode	X	X	X	X
System High Security Mode	X	X	X	S
Compartmented Security Mode	X	X	S	S
Multilevel Security Mode	X	S	S	S

X – All information on the system, S – Some information on the system

The chain-of-evidence are part of the Digital Investigation Process needed to preserve the integrity of the evidence from the moment it is identified and prepared for use until the case is disseminated as shown previously in Table I. Other than that, the evidence has to satisfy two tests as mentioned by Peter Sommer in 1997, which are *admissibility* and *weight*. Admissibility means that, the evidence must follow the legal rules which are applied by a judge while weight means the evidence must be understood by, and be sufficiently convincing to the Court of Law. Due to the large amount of network traffic to be managed and protected as evidence, a security model which describes steps taken to achieve a secure and reliable storage was considered..”

1.3. Defensive Evidence Model

In order to achieve security in the forensics system, we define our proposed DEM with the security mode mentioned earlier. A Dedicated Security Mode required the user to sign for non-disclosure agreement and proper clearance before being allowed to access. Other than that, a forensic analysis procedure might need the evidence to be analyzed frequently on the basis of investigating and required a formal verification. We summarize the feature of each model compared from aDEM perspective in Table 3. The security mode characteristic was defined as follows **a**-non-disclosure agreement, **b**-proper clearance, **c** - formal access approval, **d**-need to know. The table was composed to fit the models mentioned earlier. The characteristic of each model was closely defined to support the following characteristics; *confidentiality*, *integrity, availability and authorization.*

Phase 1 Preparation-According to the proposed phase by S.R.Selamat mentioned earlier in Table 1, the early phases of conducting investigation involve the process of preparing the case. However, no safety measures are needed during preparing the case as there is no evidence needed to be protected. Preparation only involves identifying the case and verity the witness to start evidence collection.

Table 3. Mapping of Security Models and Features of DEM

Model	**Features of DEM**				
	Phase 1	***Phase 2***	***Phase 3***	***Phase 4***	***Phase 5***
Bell-LaPadula		a,b	a,b		b
Biba		a,b,c	a,b,c	d	b
Clark-Wilson		a,c	a,c	c,d	b
Goguen-Meseguer		a,c	a,b,c		b

The proposed workflow of Digital Investigation were based on work by Mark C. Davis[11] as shown in Figure 2. The need to identify the role of user should be done as early as receiving the case.The case will be open for investigation if there are victims and witnesses. We shall label the role involve in this phase as V_n, W_n, I_n for the victim, witness and investigators respectively.

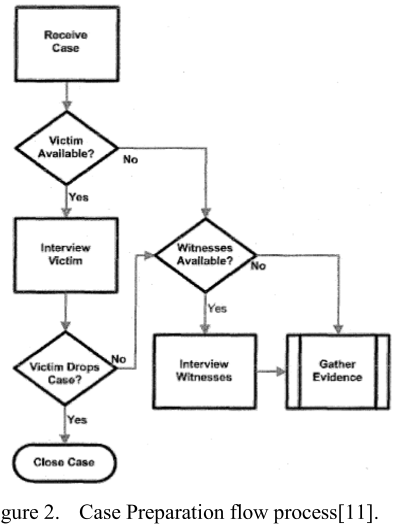


Figure 2. Case Preparation flow process[11].

Phase 2 Collection and Preservation-In the second phase, each model is involved in the confidentiality of the evidence being collected and preserved. The usersneed to build up the confidentiality of the evidence by signing the Non-Disclosure Agreement which prohibits them from exposing the evidence collected. However, Bell-LaPadula and Biba Model is the only model that needs a proper clearance to access the collected evidence which means that, the level of clearance of the I_n will increase with authorities to collect and handle the evidence and there is no clearance given to the V_n and W_n to access their own belongings as the objects were already being restricted from access. We identified the investigators involve with clearance High, Medium and Low, thus the investigators will be I_H, I_M, $I_{L.}$

While the clearance is needed to collect and preserved the evidence in Bell-LaPadula and Biba model, formal request approval were mentioned in other models which makes the possibility of the evidence to be revised if approved. This is because in digital investigations, there are possibilities of the evidence to be moved and transferred to a different location, and the integrity of the evidence will be questioned if there are users who access the evidence without approval. Thus, the user who needs to do this kind of work would be from the Courts either the Lawyer, Jury or the Judge. We identified this personal as $C_{n.}$T

Phase 3 Examination and Analysis-This phase involves the process to examine and analyzethe evidence collected. The use of database system is needed to store the evidence and the process to insert and retrieve the evidence from the database would require higher insertion and retrieval rate for examination and analysis. However, the problem of having high security would affect the performance of the database, as mentioned by U Mattsson in 2005. The focus of having security in database using encryption is very practical to protect the integrity of data stored, but will cost more on the resources to store and for handling the key for encrypting [12]. However, Mattsson proposed the use of a security catalog which is similar to traditional system catalog but with two security properties.

1. It can never be updated manually by anyone
2. Its access is controlled by a strict authentication.

DEM will be using these security properties where the evidence stored inside the database will have restrictions on the access and requires for formal access approval to access the stored evidence. There will be no access for user to analyze or conduct any experiment on the evidence. There will be three databases created for the purpose of storing the evidence, and they are Collection Database, Analysis Database and Presentation Database as shown in Figure 3. Collection database will store the original data collected for the purpose of backup while the analysis database will be where the analysis and experimenting are conducted. The last database will hold the presentation data for Courts of Law.

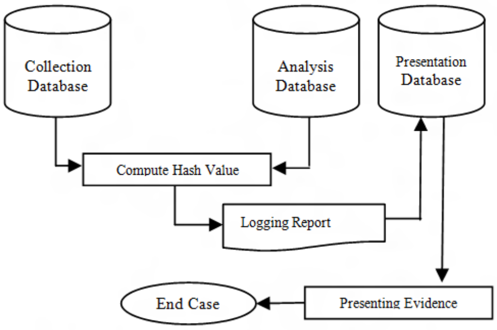


Figure 3. Database design for analyzing and presenting evidence.

Phase 4 & 5 Presentations and Reporting Disseminating the evidence- The last phase will be very crucial to the whole forensics investigations. However, the evidence presented will be verified by computing the hash value from databases, Collection database and Analysis database. The value and reporting will be generated and stored in the presentation database before retrieval for presentation in Courts of Law. The proposed model will require proper clearance for the evidence to be retrieved. In this case, the investigators, I_n will need proper clearance to access the evidence and the report will provide all the analysis and information relating to the crimes.

1.4. Attack Analysis

Defensive Evidence Model was identified with several users who have access to the system in collecting, analyzing and presenting the evidence. There are three types of attack involving evidence storage that are misused of access, defense bypass and access control failure. The worst scenario that could happen would be defending attacks that comes from inside the organization and from those who are given trust and yet with or without intentions, tampered the evidence.The attack on DEM is unavoidable if the attacker has intention to damage the evidence. But due to every single action will be recorded according to the security features, the threats will be logged. However, the entire process of investigations needed to be open report, and nothing will be hidden from other users or Courts of Law, if requested for more details on how the evidence was retrieved and who is the last person accessing the evidence. DEM will provide the entire details for viewing. Other than that, if the attack comes from insider, DEM will have the non-disclosure agreement referred as there should not be any bad intentions to damage the evidence from inside and everything will be recorded as well.

The second type of attack to the evidence storage is the defense bypass, where all the security perimeters set up by the administrator for the hardware and software protection will be manipulated or closed by the attackers. DEM with the security features of proper clearance will not allow random user accessing the evidence if they have no right to do it in the first place. Confidential information will not be easily retrieved and the user is required to have clearance even when presenting the evidence. The last attack involves the error of the system that was not noticed by the system administrator. This is the unexpected situation whereby the availability of the evidence might be compromised as such during blackout or power failure. Other failure is when the system allows access to user without any error during validation. The authorization is important for allowing unknown user or user with formal access approval. Several subjects and objects were defined based on the user and the phases involved in a forensics investigations. We summarize each user in the following Table 4.

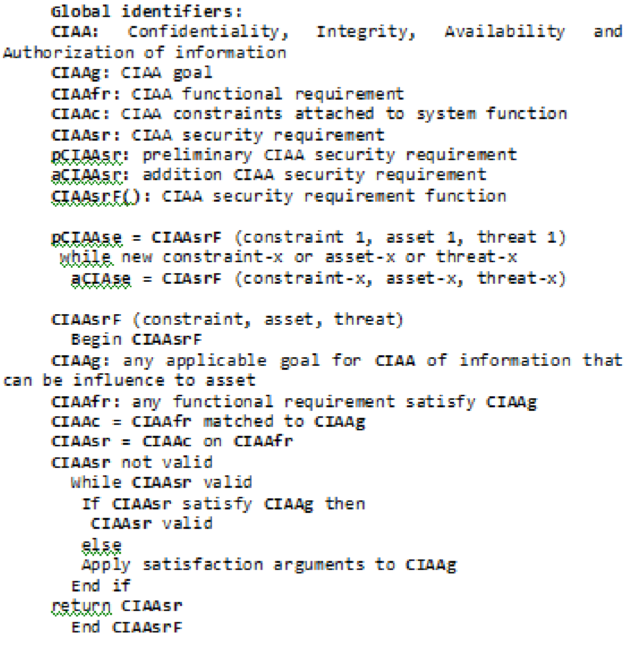
Table 4. User Identification in DEM

V_n, W_n, I_n	Victim, Witness and Investigators
I_H, I_M, I_L.	Investigators from High, Medium Low Clearance
C_n.T	Lawyer, Jury or the Judge.

1.5. Evaluation of Dem

In order to evaluate our DEM, we adapt the usage of a regular development life cycle process. The reason for choosing this development life cycle is because of the evaluation process, which can help to determine which Confidentiality, Integrity, Availability and Authorization requirements have a significant impact, when threats activate. Alfaro et al[13] evaluate these requirements for a particular threat where the confidentiality has high motivation, impact, critical risk, and it can be solvable, more than integrity and availability.

To define CIAA requirements, we use pseudo code to apply satisfaction arguments to CIAA goals, and exploitation iteration code to generate additional CIAA security requirements, as shown in Figure 4. First, we set preliminary goals, and later if we add fresh constraints, assets, or found or predict a new threat, in this case, we generate addition goals that when security requirements changed, the security goals may need changing[14].



```
    Global identifiers:
    CIAA:  Confidentiality,  Integrity,  Availability  and
Authorization of information
    CIAAg: CIAA goal
    CIAAfr: CIAA functional requirement
    CIAAc: CIAA constraints attached to system function
    CIAAsr: CIAA security requirement
    pCIAAsr: preliminary CIAA security requirement
    aCIAAsr: addition CIAA security requirement
    CIAAsrF(): CIAA security requirement function

    pCIAAse = CIAAsrF (constraint 1, asset 1, threat 1)
     while new constraint-x or asset-x or threat-x
      aCIAse = CIAsrF (constraint-x, asset-x, threat-x)

    CIAAsrF (constraint, asset, threat)
      Begin CIAAsrF
    CIAAg: any applicable goal for CIAA of information that
can be influence to asset
    CIAAfr: any functional requirement satisfy CIAAg
    CIAAc = CIAAfr matched to CIAAg
    CIAAsr = CIAAc on CIAAfr
    CIAAsr not valid
      While CIAAsr valid
       If CIAAsr satisfy CIAAg then
        CIAAsr valid
       else
       Apply satisfaction arguments to CIAAg
      End if
    return CIAAsr
      End CIAAsrF
```

Figure 4. Identify CIAA requirements

1.6. Results and Analysis

The core element for forensics system is to gain full security assurance which is iterative analysis for vulnerabilities. There are three phases as shown in Figure 5 for vulnerability analysis. The three phases are designing suitable documents for security requirements, realizing information from vulnerabilities to satisfy design documents, and running to analysing attributes of system and security control. These phases will change according to development life cycle of the system.

As shown in Figure 4, the use of a tree structure to numerate threats that use critical asset and process as root nodes, and followed by analyzing vulnerabilities that concentrate for many factors, such as system hardware, software, artificial factor, policy and procedure. All system threats will be identified in a significant way through testing and traversing all vulnerabilities according to CIAA security requirement[15].

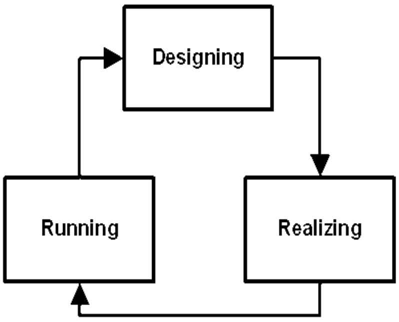


Figure 5. Analysis for vulnerabilities.

1.7. Conclusion

The increasing number of cyber-crimes along with technological advancement has been serious issues to look into. The number of cases being reported keeps increasing each year, making the law enforcement held responsible to conduct investigations while preserving the collected evidence. However, most of the studies are related to mechanisms and framework in Digital Forensics and less are discussing on Network Forensics especially in keeping the evidence safe. Storing network evidence in a proper ways is crucial as network evidence is unpredictable.

The lack of reliable storage for storing large amounts of network evidence was discussed in this paper. The development of Defensive Evidence Model was discussed from two different aspect, the attack analysis and the analysis of Security Requirement Process to determine if the used of Confidentiality, Integrity, Availability and Authorization fulfill the created model. Defensive Evidence Model is target to prevent threats and to protect evidence as assets and work parallel with system components to avoid any drastic changes on system functionality. Furthermore, DEM was analyzed from 3 types of attack that could happen, and the analysis showed DEM functional to handle misused of access, defense bypass and access control failure.

For our future work, the use of Security Requirement Process to validate the Defensive Evidence Model will be briefly studied. Alternatively, the use of database model to store evidence is a essential for forensic evidence system thus we are going to adapt DEM using column-based database to get higher insertion rate and retrieval rate in storing and analyzing the evidence.

Acknowledgements

We would like to thank the members of Security Research Group (SRG), USM for their helpful discussions and suggestions.

References

1. (MyCERT), M.C.E.R.T., MYCERT 4TH QUARTER 2011 SUMMARY REPORT, in e-Security. 2011, CyberSecurity Malaysia. p. 1-2.
2. Cho, C.Y., et al., Network forensics on packet fingerprints. Security and Privacy in Dynamic Environments, 2006. **201**: p. 401-412.
3. Wang, H.-M. and C.-H. Yang. Design and Implementation of A Network Forensics System for Linux. 2010: IEEE.
4. Qaisi, A., Network Forensics and Log Files Analysis: A Novel Approach to Building a Digital Evidence Bag and Its Own Processing Tool, in Department of Computer Science and Software Engineering. 2011, University of Canterbury. p. 157.
5. Carrier, B.D., A Hyphotesis-based Approach to Digital Forensic Investigations, in Center for Education and Research in Information Assurance and Security. 2006, Purdue University: West Lafayette. p. 190.
6. Selamat, S.R., R. Yusof, and S. Sahib, Mapping Process of Digital Forensic Investigation Framework. International Journal of Computer Science and Network Security, 2008.p. 7.

7. Pladna, B., Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them, in Computer Forensics Procedures, Tools, and Digital Evidence Bags. 2008, East Carolina University.p. 8.
8. Krutz, R.L. and R.D. Vines, The CISSP Prep Guide. Gold Edition, ed. 2003, Indianapolis, Indiana: Wiley Publishing, Inc.p. 263.
9. Fisch, E.A. and G.B. White, Secure computers and networks: analysis, design, and implementation. 2000: CRC Press.
10. Arthur, K.K., Considerations Towards the Development of a Forensic Evidence Management System, in Faculty of Engineering, Built Environment, and Information Technology. 2010, University of Pretoria. p. 132.
11. Davis, M.C., A Network Based Storage Model For The Processing of Digital Evidence. 2009, The University of Tulsa.
12. Ulf T. Mattsson, Database Encryption - How to Balance Security with Performance. 2005
13. Garcia-Alfaro, J., M. Barbeau, and E. Kranakis. Security Threats on EPC Based RFID Systems. In Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on. 2008.
14. Charles, B.H., et al., A framework for security requirements engineering, in Proceedings of the 2006 international workshop on Software engineering for secure systems. 2006, ACM: Shanghai, China.
15. Hui, W., J. Zongpu, and S. Zihao. Research on security requirements engineering process. In Industrial Engineering and Engineering Management. IE&EM '09. 16th International Conference on. 2009.