Common Investigation Process Model for Database Forensic Investigation Discipline

Arafat Aldhaqm[1*], Shukor Abd Razak[2], Siti Hajar Othman[3]

[1]Faculty of Computing, Univercity Technology Malaysia, Malaysia
[2]Faculty of Computing, Univercity Technology Malaysia, Malaysia
[3]Faculty of Computing, Univercity Technology Malaysia, Malaysia

* corresponding author: Arafat Aldhaqm: arafataldoqm@gmail.com

Abstract

Current digital forensic process models are often found to be unsatisfactory due to the fact that they do not provide process model with opportunities to be actively involved database forensic investigation. This study presents common database forensic investigation process, which is proposed by reviewing a few particular digital investigation process models that have created and then identified the frequently common processes phases concentrates. Results of this study showed that with the determining of the frequently shared process, it could be easier for the new users to recognize the processes and also to serve as the basic fundamental concept for the improvement of a new set of processes. Thus, proposing this kind of process model may help to resolve the problems and difficulties associated with database forensic in general.

Keywords. Database Forensic, Forensic Artifacts, Investigation Process

1 Introduction

Database management systems are used for organizing and managing huge of data. Usually, most of organizations stored their valuable information in database systems. Nevertheless, they have been suffering and struggling in order to secure and protect their information against several of database attacks [1]. Technically, database security countermeasures are used for monitoring, detecting, preventing and auditing database systems, thus, they do not have the ability in revealing the reasons of intrusion such as who has been intruding with? When intrusion has been happened? What data that has been tampered with? Why and how did intruding happen? [2]. Therefore the cooperating between database security countermeasures and Database Forensic Investigation (DBFI) is highly recommended.

Database Forensic investigation is dealing with database contents and metadata in order to revealing database crimes [2], [3], . It reconstructs database activities from redo logs, data files, backup files and undo segment, in order to recovering database consistency and discovers malicious activities [4]. It provides many forensic techniques towards detecting, collecting, analyzing, and documenting database events, however they are reported in different resources such as the internet, books, journals, organizations and dissertations [5], [6]. DBFI has many challenges and issues such as variety of database systems architectures, and multidimensional nature of database systems, which are produced complexity, and confusion amongst investigation community [2].

Due to the lack of common database forensic investigation process model [7], the main objective of this study is to provides obvious structure which called Common Investigation Process Model for Database Forensic Investigation discipline to unifying, facilitating, and sharing database forensic investigation process knowledge amongst database users and practitioners. This model provides a pure and specific database forensic concepts and terminologies which are using through database forensic investigation. Unifying these concepts in one conceptual model will increase knowledge of users, newcomers and practitioners. Additionally, reduce the complexity and ambiguity of investigation.

2 Methods

This study utilizes Design Science Research (DSR) methodology towards propose process artifacts which is called common process investigation model for DBFI [8], [9]. Five steps are used to develop proposed model:
(a) Identify and collect the digital forensic process models that display in Table 1.
(b) Extract investigation process phases and candidate common process phases using Inverse Document Frequency (IDF).
(c) Allocate synonyms investigation process with the fit pure common process.
(d) Identify the relationships among common process phases that yields common investigation process model for DBFM which displayed in Figure 1.
(e) Validate proposed model through face valid.
Nevertheless, in this paper the Inverse Document Frequency (IDF) method to measuring the importance of a process in models collection has used [10]. IDF defines as "a statistical weight used for measuring the importance of terms in a text document collection". The document frequency (DF) of a term is defined by the number of documents in which a term appears. Hence, in this paper the authors adapted this frequency method to measuring the importance of processes in collected models which adapted as Inverse Model Frequency (IMF). However, it adapted to measuring the rank of a process in models gathering. In its simplest form, the IMF weight of a process is assigned as follows:

$$\mathbf{IMF = Log\ (N/MF)} \qquad (1)$$

Where N is the number of models in the collection, and MF is the Model Frequency of the process, i.e., the number of models in which the process appears.

3. Results and Discussion

Fourteen digital forensic investigation process models together with specific database forensic investigation process models have been identified, and collected such as M1 [11], M2 [12], M3[13], M4 [14], M5 [15], M6 [16], M7 [17] , M8 [18], M9 [19], M10 [20], M11[21], M12 [4], M13 [22], M14 [23]. Table 1 displays the comprehensive analysis of these models and their process phases. Forty three investigation process phases have extracted, reviewed and compared towards candidate common investigation processes phases. Five common investigation process phases have been selected based on their frequency and repeating in process models using IMF method which is mentioned in Section 1. In this study, the process investigation phases are divided into two parts: Pure processes and Synonym processes. Pure processes are the processes that have perfect and clear name such as identification, collection, analysis, document, preparation, and presentation, whereas the Synonyms processes are the processes that have alternative name of the pure name for example acquisition, search and identify evidence, and reconnaissance is the synonym names of the collection process phase.

Therefore, the five common investigation process phases which have been selected are: Identification, Collection, Preservation, Analysis and Presentation phase. Table 1 shows five colors which represent these phases. Hence, Red color represents the pure process phase which called Identification Process Phase including its synonyms processes such as admission, authentication, preparation, approach strategy, readiness, development, awareness, authorization, planning, notification, hypothesis, pre-analysis, incident, incident response, suspend database, setting up the evidence collection server, and incident verification, while the other colors like Green, Yellow, Blue, and Brown represent Collection Process Phase, Preservation Process Phase, Analysis Process Phase, Presentation Process Phase as well as their synonyms processes respectively. The common investigation process phases and their synonyms represent the most processes phases which probably have covered digital forensic discipline. Therefore, they can adapt to dealing with DBFI.

Practically, the authors reconcile, and improve the common investigation phases by adding mandatory and optional forensic concepts and terminologies which are required during investigation. For example, the mandatory forensic concepts and terminologies are law/regulation, database resources, investigation team, authorization, detection server, database incident, identification, preservation, and volatile and nonvolatile artifacts, whereas the optional concepts and terminologies are network resources, and OS re-

sources. Additionally, the authors allocate suitable definition for proposed common investigation process phases and then link each of which through semantic arrows to formulate initial common investigation process model that illustrates in Figure 1.

4. Conclusion

Database forensic investigation discipline does not have a common investigation process model, due to many challenges and issues. However, several digital investigation process models have been discussed and reviewed to propose common investigation process model for database forensic. Frequency based selection technique and DSR methodology are used in this paper. Our future work will concentrate on describing in details all the process investigation phases of common process model.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education Malaysia (MoHE) and Universiti Teknologi Malaysia (UTM) for funding this study under the Fundamental Research Grant Scheme (FRGS) of Grant No. PY/2014/03139 (R.J130000.7828.4F498).

References

1. Ngadi, M., R. Al-dhaqm and A. Mohammed. Detection and prevention of malicious activities on RDBMS relational database management systems. *International Journal of Scientific and Engineering Research*. 2012. 3(9): 1-10.
2. Olivier, M. S. On metadata context in database forensics. *Digital Investigation*. 2009. 5(3): 115-123.
3. Guimaraes, M. A., R. Austin and H. Said. Database forensics. *2010 Information Security Curriculum Development Conference*: ACM. 2010. 62-65.
4. Wong, D. and K. Edwards, System and method for investigating a data operation performed on a database. 2004, Google Patents.
5. Al- Dhaqm, A. M. R., S. H. Othman, S. Abd Razak and A. Ngadi. Towards adapting metamodelling technique for database forensics investigation domain. *Biometrics and Security Technologies (ISBAST), 2014 International Symposium on*. 26-27 Aug. 2014. 2014. 322-327.
6. Hauger, W. K. and M. S. Olivier. The role of triggers in database forensics. *Information Security for South Africa (ISSA), 2014*: IEEE. 2014. 1-7.
7. Fasan, O. M. and M. Olivier. Reconstruction in database forensics. *Advances in Digital Forensics VIII*. Springer. 273-287; 2012
8. von Alan, R. H., S. T. March, J. Park and S. Ram. Design science in information systems research. *MIS quarterly*. 2004. 28(1): 75-105.
9. Othman, S. H. and G. Beydoun. Metamodelling approach to support disaster management knowledge sharing. 2010.
10. Ounis, I. Inverse Document Frequency. *Encyclopedia of Database Systems*. Springer. 1570-1571; 2009
11. Pollitt, M. Computer forensics: An approach to evidence in cyberspace. *Proceedings of the National Information Systems Security Conference*. 1995. 487-491.
12. Kruse II, W. G. and J. G. Heiser. *Computer forensics: incident response essentials*: Pearson Education. 2001
13. Palmer, G. A road map for digital forensic research. *First Digital Forensic Research Workshop, Utica, New York*. 2001. 27-30.
14. Reith, M., C. Carr and G. Gunsch. An examination of digital forensic models. *International Journal of Digital Evidence*. 2002. 1(3): 1-12.
15. Carrier, B. and E. H. Spafford. Getting physical with the digital investigation process. *International Journal of digital evidence*. 2003. 2(2): 1-20.
16. Ciardhuáin, S. Ó. An extended model of cybercrime investigations. *International Journal of Digital Evidence*. 2004. 3(1): 1-22.
17. Baryamureeba, V. and F. Tushabe. The enhanced digital investigation process model. *Proceedings of the Fourth Digital Forensic Research Workshop*: Citeseer. 2004.
18. Fowler, K. *SQL Server Forenisc Analysis*: Pearson Education. 2008
19. Köhn, M., M. S. Olivier and J. H. Eloff. Framework for a Digital Forensic Investigation. *ISSA*. 2006. 1-7.

20. Freiling, F. C. and B. Schwittay. A Common Process Model for Incident Response and Computer Forensics. *IMF*. 2007. 7: 19-40.
21. Perumal, S. Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security*. 2009. 9(8): 38-44.
22. Kohn, M. D., M. M. Eloff and J. H. Eloff. Integrated digital forensic process model. *Computers & Security*. 2013. 38: 103-115.
23. Tripathi, S. and B. B. Meshram. Digital Evidence for Database Tamper Detection. *Journal of Information Security*. 2012. 3: 113.

Table 1. Common Analysis of Digital Forensic Process Models

ID	ProcessModel	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	MF	IMF
1	Acquisition	v	v													2	0.845
2	Identification	v			v	v					v					4	0.544
3	Collection			v	v			v					v	v	v	6	0.367
4	Evaluation	v														1	1.146
5	Admission	v														1	1.146
6	Authenticating		v													1	1.146
7	Analysis		v	v	v					v	v		v	v		7	0.301
8	Preservation			v	v								v		v	4	0.544
9	Examination			v	v			v								3	0.669
10	Presentation			v	v			v	v			v				5	0.447
11	Decision			v												1	1.146
12	Preparation				v				v			v			v	4	0.544
13	Approach strategy				v											1	1.146
14	Returning evidence				v											1	1.146
15	Readiness					v	v									2	0.845
16	Deployment					v	v									2	0.845
17	Review					v	v									2	0.845
18	Traceback						v									1	1.146
19	Dynamite						v									1	1.146
20	Awareness							v								1	1.146
21	Authorization							v								1	1.146
22	Planning							v			v					2	0.845
23	Notification							v								1	1.146
24	Search and identify evidence							v								1	1.146
25	Transport of evidence							v								1	1.146
26	Storage of evidence							v								1	1.146
27	Hypothesis							v								1	1.146
28	Proof/Defense of hypothesis							v								1	1.146
29	Archive storage							v			v					2	0.845
30	Investigation								v							1	1.146
31	Pre-analysis									v						1	1.146
32	Post-analysis									v						1	1.146
33	Reconnaissance										v					1	1.146
34	Transport & Storage										v					1	1.146
35	Proof and Defense										v					1	1.146
36	Incident											v				1	1.146
37	Incident response											v				1	1.146
38	Suspend database operation												v			1	1.146
39	Reconstruct												v			1	1.146
40	Restore database integrity phase												v			1	1.146
41	Setting up the evidence collection server													v		1	1.146
42	Incident verification														v	1	1.146
43	Report														v	1	1.146

Figure 1. Common Database Forensic Investigation Process Model