Research Journal of Applied Sciences, Engineering and Technology 12(4): 386-394, 2016
DOI: 10.19026/rjaset.12.2377
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: February 6, 2015 Accepted: March 12, 2015 Published: February 25, 2016

Research Article

Conceptual Investigation Process Model for Managing Database Forensic Investigation Knowledge

Aarafat Aldhaqm, Shukor Abd Razak, Siti Hajar Othman, Abdulalem Ali and Asri Ngadi
Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Johor, Malaysia

Abstract: Database Forensic Investigation (DBFI) discipline has been utilizing in identifying, collecting, preserving, analyzing, reconstructing and documenting database crimes. DBFI knowledge has scattered anywhere and has not ever an obvious structure to managing it. This study makes survey of several DBFI knowledge process models, algorithms, methods, artifacts and tools offered till date. The functionality of many DBFI analysis algorithms and several DBFI artifacts available for forensics investigator are discussed. The DBFI challenges and issues are highlighted. The significance of this study is that it presents conceptual investigation process model and an overview on DBFI knowledge covering algorithms, process models, methods and artifacts forensics, which will be very much useful for DBFI users, practitioners and researchers in exploring this upcoming and young discipline.

Keywords: Database forensic, DBMS, forensic artifacts, nonvolatile artifacts, process model, volatile artifacts

INTRODUCTION

Database systems have been storing, sorting, managing and retrieving huge of critical and sensitive data. Confidentiality, integrity and availability of database systems are highly required against database crimes. Database crimes are insider or outsider malicious activities which are threaten integrity, confidentiality or availability of database (Ngadi *et al*., 2012). Nevertheless, database security measures that are providing detection and prevention of database systems are not full enough in discovering most of database crimes and tracing their malicious methodologies (Ngadi *et al*., 2012). Database security products like alerting, tracing and auditing tool are generalized and looking for possible harmful behaviors. They are monitoring data against database crimes. These crimes may be handled by database forensic investigation (Olivier, 2009).

The DBFI discipline is needed for identifying, collecting, preserving, analyzing, reconstructing, recovering and documenting database crimes. It is a branch of digital forensic investigation that is dealing with database contents, metadata, log files, data files and memory data in order to create a timeline, relationship or recover relevant (Cohen, 2012). However, DBFI knowledge are scattered anywhere in internet, books, journals, online databases, dissertations and organizations (Al- Dhaqm *et al*., 2014).

The objective of this study is to providing overview of DBFI knowledge elements such as process models, detection and analysis algorithms, forensic artifacts, forensic methods and forensic investigation tools. In addition, propose conceptual investigation process model in order to managing, structuring and sharing this knowledge amongst database forensic investigation community.

MATERIALS AND METHODS DATABASE CRIMES

Most of organizations have been struggling and suffering in protecting their sensitive information of suspected intentional or unintentional activities. Tampering of information may lead to failure to meeting of information security primary goal which called confidentiality, integrity and availability (Williams III, 2006). Many database crimes had been happening during last decade which had been breaching of database systems. Table 1 shows these crimes. Obviously, it shows that corporations have not taken seriously their information security goals (Natan, 2005), therefore, most of implemented database security products may or may not be capable in protecting databases of database crimes.

Thus, investigations procedures like DBFI are highly recommended.

Database forensic investigation knowledge history: The DBFI field has received a little of researches and attentions yet, due to complexity and multidimensional nature of the DBMS (Fasan and Olivier, 2012; Williams III, 2006) which have leaded to many issues like lack of: knowledge and training (Guimaraes *et al*.,

Corresponding Author: Arafat Aldhaqm, Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Johor, Malaysia

Table 1: Database crimes

Year	Database victim	Details
2000	Retailer's database	The Hacker who's called Maxus stole credit card numbers and attempt to fraud money from the retailer. When his requests were refused, he published thousands of customer's credit card details on the internet (Natan, 2005).
2000	Online Retailer Egghead.com customer database	Approximately 3.5 million credit card numbers were stolen (Natan, 2005).
2001	Bibliofind, a division of Amazon	The attackers stole approximately 100, 000 credit card details and also after reached database, they maintained access to the database for a few months (Natan, 2005).
2001	Web site's Banks	Federal Bureau of Examination (FBI) reported that Russian and Ukrainian hackers had attacked more than fifty web sites of banks (Natan, 2005).
2001	Playboy.com	The credit card numbers of customers were stealing and the attackers send emails to them with their credit card information (Clarke, 2012).
2001	Indiana University	The attackers had been reached twice and stolen the sensitive information such as social security numbers and addresses.
2002	Guess.com	The attackers used SQL injection and stolen more than 200, 000 credit card number (Clarke, 2012).
2003	PetCo.com	The attackers used SQL injection and stolen more than 500, 000 credit card number (Clarke, 2012).
2005	Master card	More than 40 million credit cards number were stolen during security incident.
2005	Guidance software	The developers of company discovered the malicious SQL injection flaw in their database server and lead to stole 3, 800 financial records of customers (Clarke, 2012).
2006	Virginia's electronic prescription drug database hostage	The attackers claimed $10 million as ransom. They reached 35 million prescription drug records in the online database.
2007	U.S. discount retailer TJX	45.7 million Of credit and debits cards were stolen from their database during incident security (Suffern, 2010).
2007	United Nations website	The transgressors attacked united nation websites vie vulnerabilities of SQL rejection in order to display the anti-United State message.
2009	Terrorist screening database	One of the TSA Colorado Springs Operation Center data analyst was terminate and charges for his tampering in the terrorist screening database (Ericka, 2010)
2011	Sony Corporation	Around 77 million users' credit card details and 100 million account details have been compromised by attackers (Baker and Finkle, 2011).
2011	North Atlantic Treaty Organization	Unknown hackers attacked the organization servers and stolen 1 gigabyte of restricted and sensitive information (Montalbano, 2011).
2012	Environment Protection Agency Database	The superfund program of the database of agency such as security social number, bank routing number and home addresses for 7, 800 current and past employees has attacked by unknown hackers (Kaplan, 2012).
2012	University of Georgia	The social security number, employee's names and sensitive information for 8500 former employees have been breached by intruders during 2012. And also in 2011 the university officials have been disclosed the personal information for 18, 000 staff and faculty members and posted on web server for three years (Shearer, 2012).

2010), perfect tools and techniques (Olivier, 2009), generic process model and forensic tool (Fasan and Olivier, 2012), obvious structure to manage DBFI knowledge (Al-Dhaqm *et al*., 2014), furthermore volatility of collected data (Fowler, 2008), huge of collecting and analyzing data, moreover database root kits (Reith *et al*., 2002). However, these challenges and issues have discussed by Al- Dhaqm *et al*. (2014). Mostly, the developed researches have been concentrated on practical level (Litchfield *et al*., 2005; Olivier, 2009), however probably have not focused on underlying model. Moreover, they have not ever been presenting generic process investigation model (Olivier, 2009).

Figure 1 shows DBFI domain knowledge, which includes specific DBFI process models, detection and analysis algorithms, forensic artifacts, tools and methods.

Database forensic investigation process models: Several specific DBFI process models have been developed to dealing with DBMS which are illustrate in Fig. 1. However, currently DBMS have not being generic investigation process model (Fasan and Olivier, 2012). For example specific investigation process model has developed by Wong and Edwards (2004), which has been using to discovering Oracle database suspected activities such as SQL injection attacks and fraud credit cards. It has been utilized Oracle built-in features such as flashback, recycle bin, redo log, undo log, SQL cache and auditing trails, furthermore some network detection techniques such as firewall and IDS.

Typically they are using for collecting and analyzing suspected activities and revealing crimes reasons. Additionally, other investigation process model has been developed by Tripathi and Meshram (2012) to revealing Oracle database crimes. It was totally based on series forensic practical techniques (Litchfield, 2007a 2007b, 2007c, 2007d, 2007e, 2007f, 2008) which have developed to dealing with Oracle database crimes. Also, MS SQL database server has specific investigation model which developed by Fowler (2008). It consists of fiver investigation phases such as investigation preparation, incident verification,

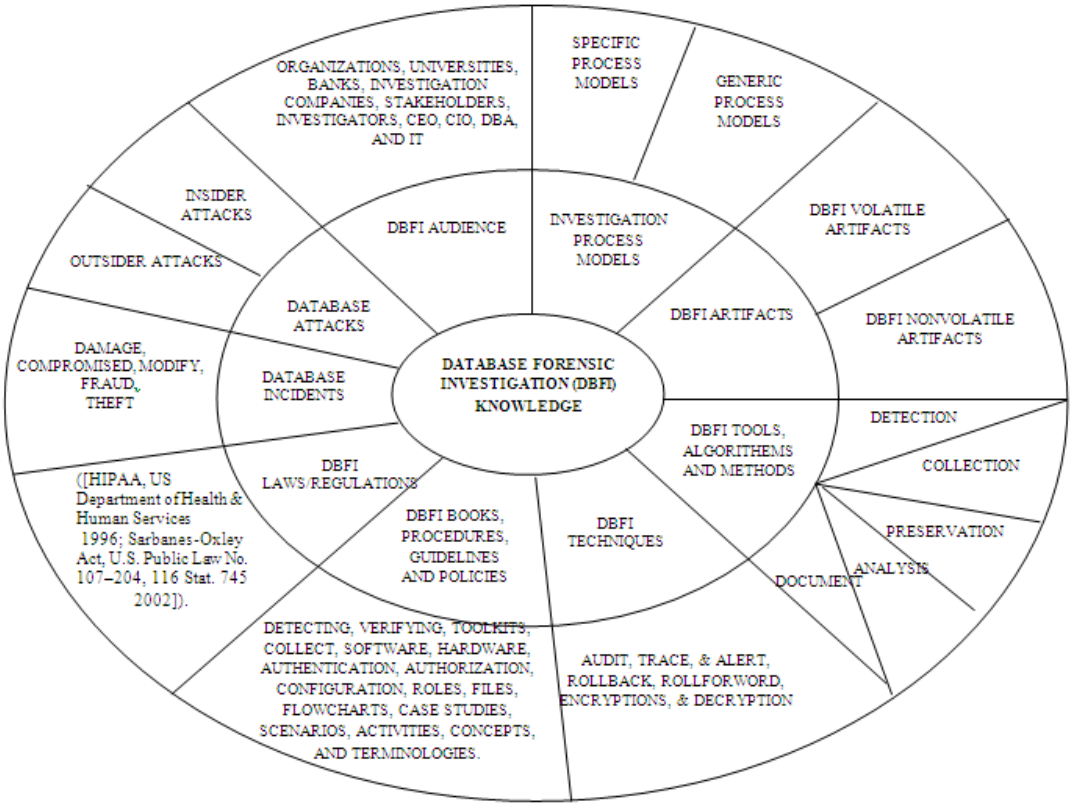

Fig. 1: Database forensic investigation knowledge

artifact collection, artifact analysis and report. It is utilizing in collecting and analyzing database volatile and nonvolatile artifacts, for example but not limited Transaction logs, SQL cache memory and Data cache memory. Furthermore, MySQL database server has particular investigation process framework (Khanuja and Adane, 2012). It consists of four investigation phases for example identification, collection artifacts, analysis artifacts and report. MySQL database built-in features such as mysqldump (database backup program), mysqlaccess (client for checking access privileges), myisamlog (display MyISAM log file contents), myisamchk (myisam table maintenance utility), mysqlbinlog (utility for processing binary log files) and mysqlbinlog hex dump format have used in identifying, collecting and analyzing database crimes. Similarly, investigation process model was developed to dealing with enterprise environment (Son *et al*., 2011). It consists of three investigation process stages: server detection, collection data, investigated collected data. It concentrated on detection methods, staff interview and employees to detecting database server, database crimes, collecting and analyzing data and revealing suspected malicious activities.

Therefore and regarding to what discussed in this paragraph, it seems clearly that the DBMS lacks of generic investigation process model (Al-Dhaqm *et al*., 2014; Fasan and Olivier, 2012; Olivier, 2009). Usually, DBFI examiners have used specific forensic detection and analysis forensic algorithms, forensic techniques and tools along with DBFI process models.

Database forensic investigation algorithms: DBFI has some detection and analysis forensic algorithms which are using in detecting database tampering and analyzing suspect's events based on timestamp of events. Detecting database tampering algorithm was developed by Snodgrass *et al*. (2004). It based on strong cryptography one way hash function, master secure database, notarization services and validator which are using to detecting undesired activities in log files. The cryptography one way hash function is using in hashing transactions and sending it to notarization services. Notarization services are responsible of storing hash values and generating Notary ID and sending it back to master secure database. The master secure database stores hashed values and Notary ID. Thus, if doubting has occurred against suspect's events, then validator is triggering. Validator is responsible of rehashing original transactions and comparing it along with Notary ID which are storing in master database. The results of comparing will decide whether database has tampered or not. In case of tampering happened, then series of database forensic analyses algorithms like Monochromatic algorithm, Red Green Blue algorithm (RGB) (Pavlou and Snodgrass, 2008), Red Green Blue

Yellow algorithm (RGBY) (Pavlou and Snodgrass, 2008), a3D algorithm (Pavlou and Snodgrass, 2008) and Tile bitmap algorithm (Pavlou and Snodgrass, 2010) are required to revealing: Who has been tampered with? When tampering has been happened? What data which has been tampered? Why data has been tampered? How tampering has been done?, therefore Monochromatic analysis algorithm it uses only a single hash chain for the given instant to identify the tampering data, whereas RGB Algorithm is producing new types of hash chains which are indicating three colors like red, green and blue. All these three chains are parallel synchronized to commit the transactions in database. Moreover, the RGBY algorithm was proposed for improves RGB algorithm by adding another hash chain called 'Y' which denotes yellow color. This extra hash chain is taken care of notarization service of transactions. Also, a3D algorithm is one of the most advanced algorithms as it does not lay continuously for a fixed pattern of hash chains over the database. Instead of this the length of partial chains keeps increasing as the transaction time increases. Finally, Tiled Bitmap Algorithm introduces the notion of a candidate set (all possible locations of detected tampering) and provides a complete characterization of the candidate set and its cardinality. In fact, these algorithms may assist examiners in extracting and analyzing evidences from database forensic artifacts.

Database forensic investigation artifacts: Initially, database forensic artifacts assist examiners in detecting database crimes regardless of their varying and heterogeneous properties. An artifact defines as "An object that has been intentionally made or produced for a certain purpose" (Eessaar, 2006). In computers, artifacts may refer to data files, log files, event logs, registry values, memory caches, configuration files, settings and so on (Carvey, 2009). Therefore, database forensic artifacts are considering crucial resources for examiners (Fowler, 2008), thus they classify into two parts based on their properties: volatile and nonvolatile artifacts (Al-Dhaqm *et al*., 2014). Volatile artifacts are objects that are carrying volatile or fragile data such as data cache, undo cache, shared cache, data dictionary cache and SQL cache, whereas nonvolatile artifacts are objects which are carrying nonvolatile data for example but not limited log files, data files, transaction log, authentication and authorization files, auditing files, alert and trace files and configuration files. Hence, variety of database systems may have made database artifacts different and heterogeneous; however they have same functionalities in most cases. For example the names of the data cache, SQL cache and transaction logs may vary between database management systems, nevertheless conceptually, they perform the same functions regardless of the database management system (Suffern, 2010). Structuring, managing and unifying database forensic artifacts concepts are highly required. Figure 1 shows some database forensic artifacts. Actually, these artifacts need forensic methods and tools to dealing with.

Database forensic investigation tools: Database forensic investigation discipline has not been perfect generic forensic tool yet (Al-Dhaqm *et al*., 2014; Fasan and Olivier, 2012). However, some of database security utilities such as Log Miner in an Oracle (Wright, 2005), SQL Trace and SQL Profiler in MS SQL server and ProfilerEventHandler in MySQL (Khanuja and Adane, 2012) are using to achieve somehow forensic tools tasks. The Log Miner has been using to reconstructing actions taken on an Oracle database even when auditing features have been turned off. However, it is insufficient for a forensics analysis due to anomalies that revealed during forensic analysis (Al-Dhaqm *et al*., 2014; Fasan and Olivier, 2012). Database activity can be audited through a SQL trace in MS SQL server which is one of the security policies. This is an interface made available through extended stored procedures to identify poorly running SQL statements and to debug other performance problems (Khanuja and Adane, 2012). An application SQL Profiler collects the events. But only SQL Trace cannot be relied to monitor database. It is said that even Microsoft discourages the use of SQL Traces on a production system, because when enabled it can consume memory, CPU cycles and disk space. Also SQL Trace does not audit or monitor systems on continuous basis. The traditional auditing system does not have intelligence built into it. It does not support filtering conditions. No amendment is possible to trace to what, when, or who is being audited. It is difficult to trace malicious activity. It is said that SQL Trace is great at amassing a huge amount of data, but is inadequate in finding the "needle in the haystack" that is evidence of malicious activity (Khanuja and Adane, 2012). Similarly in MySQL 'Information_Schema' table provides access to database metadata. The ProfilerEventHandler class in MySQL implements the interface that is used to handle profiling and tracing the events. Nevertheless, the DBFI has some free and commercial tools which have been offering by industrial community such as SQLite Forensic Reporter, Scuba by Imperva, Android Data Extractor Lite (Spreitzenbarth *et al*., 2012) and User Behavior Analysis (Qian *et al*., 2014). In addition, DBFI has several forensic methods which have been using to revealing details of database crimes.

Database forensic investigation methods: Database forensic investigation field has particular forensic methods which are using in detecting, collecting, protecting, analyzing and recovering database events. Usually, forensics methods are working a long with

DBFI process models. Thus, investigators/examiners team should be identifying investigation requirements concepts such as law/regulations, policies, authorizations and authentications resources, database resources, OS resources, network resources, investigation environment, investigation techniques and investigation teams. These forensic methods are working sequentially to get desired results.

Database forensics detection methods: Are multipurpose and utilizing to detecting database crimes and their relevant. They are using in detecting crimes, permanent database, covert database, type of database, host server where is database has been resided, database accounts, privileges, auditing files, tracing files, logging files and so on. Moreover, in this stage the investigator may be detecting which kind of database tampering type of attack, attack time and attack resources. In general, the forensics methods that are using in detecting database crimes were developing by Fruhwirt *et al*. (2010, 2012), Frühwirt *et al*. (2013), Lee *et al*. (2007, 2008), Ngadi *et al*. (2012), Son *et al*. (2011) and Tripathi and Meshram (2012). Obviously, DBFI has not pure detection forensic method yet. Actually, most of them are specific methods. Consequently, in this stage the initial incident may detected and the resources which have been identified must be collected, saved and documented.

Database forensics collection methods: Are using in grasping volatile and nonvolatile data which are identified by database forensics detection methods. Thus, they classified in to three methods (Fowler, 2008): Live, dead and hybrid acquisition. The Live acquisition methods which are using in collecting data from volatile artifacts such as SQL cache, data cache, shared cache and so on (Fowler, 2008). Consequently, the skilled and experienced investigation team are required, due to the live acquisition achieved when system is going on and on the other hand the volatility of some volatile data is highly (Al-Dhaqm *et al*., 2014; Fowler, 2008). Nevertheless, the dead acquisition methods are using in collecting the nonvolatile data such as log transactions, data files, log files, auditing file etc. The hybrid acquisition methods combines key elements of both live and dead acquisition methods to give you the best of both worlds (Fowler, 2008). In simpler term, hybrid acquisition can be viewed as a typical dead acquisition that is performed after the live acquisition of volatile data. The Database forensics collection methods are (Azemovic and Music, 2010; Fowler, 2008; Jin and Osborn, 2007; Son *et al*., 2011; Tripathi and Meshram, 2012; Wong and Edwards, 2004) which are displaying on Fig. 1. Keep in the mind, that all of the database forensic collection methods are specific techniques which have not developed for pure investigation forensic. Finally, collected data must be redundancy copied, documented and hashed avoiding of any damaging or altering when moving to analyzing stage.

Database forensic preserving methods: Are securing mechanisms which are providing strong functions in protecting collected data against intentionally or unintentionally activities either during investigation task or transportation. Securing mechanisms are cryptography strong one way hash functions which are using in checking authentic/integrity data (Wong and Edwards, 2004). Such as hash functions, including SHA-1 and MD5. Preserved data should be redundant and documented to protecting it against physical or digital damage. The database forensic preserving methods are founding in Azemović and Mušić (2009), Basu (2006), Kambire *et al*. (2015) and Snodgrass *et al*. (2004). Therefore, the main purpose of these methods is to providing original data for analyzing without tampering.

Database forensic analysis methods: Database management systems provide specific build-in utilities which are using to reconstructing and analyzing database events and then restoring and recovering database activities. These methods may give it name as database forensic analyzing methods based on their functions. The suspected database events are reconstructing/rebuilding using undo log segment or redo log files a long with history data like backup pieces and archived pieces. Undo segment is volatile artifact/memory which is holding uncommitted transactions, that have been not moved database yet, whereas redo log file is nonvolatile artifact that is holding committed transaction, that moved database (Wong and Edwards, 2004). Both of them are using for rebuilding database activities through rollback or roll forward techniques (Wong and Edwards, 2004). Consequently, the reconstructed events are matching and comparing along with normal transactions times using series of database forensics analysis algorithms which developed by Pavlou and Snodgrass (2008, 2010). These algorithms are using in revealing crimes details. Thus, database integrity is restoring to last failure/tampering point, using an incomplete clean backup pieces and sequence online archive redo log pieces (Wright and Burleson, 2008). Several specific database forensic analyzing methods have been offering for reconstructing activities like (Fasan and Olivier, 2012; Fruhwirt *et al*., 2012; Frühwirt *et al*., 2013; Wright, 2005), while others have been offering as well for recovering database damaged, compromised, or changed like (Choi *et al*., 2013; Haerder and Reuter, 1983; Wu *et al*., 2013; Xu *et al*., 2013). Optionally, take in the mind, the various DBMS built-in utilities may be using for reconstructing and recovering database

activities, for example but not limited flashback and recycle in an Oracle language. Finally, the results must be documented and submitted to top management.

RESULTS AND DISCUSSION

Through aforementioned reviewed above of the DBFI knowledge, it seems obviously that DBFI lacks of obvious structure to facilitating, reusing, unifying, sharing and managing DBFI knowledge. However, this study proposes conceptual investigation process model which including five investigation process phases namely Identification phase, Collection Phase, Preservation Phase, Analysis Phase and Presentation Phase. Actually, fourteen digital forensic investigation process models have been reviewed and analyzed to propose this model. Table 2 displays these process models.

The conceptual investigation process model which illustrates in Fig. 2, considers as a guide for database forensic investigators. Mostly, it provides somehow greatest of investigation concepts which investigators may need it during investigation mission. Most of the DBFI knowledge concepts and terminologies are offering in this conceptual process model. In fact, this process model is not only for special investigators; however it may offers for beginners and new comers as well.

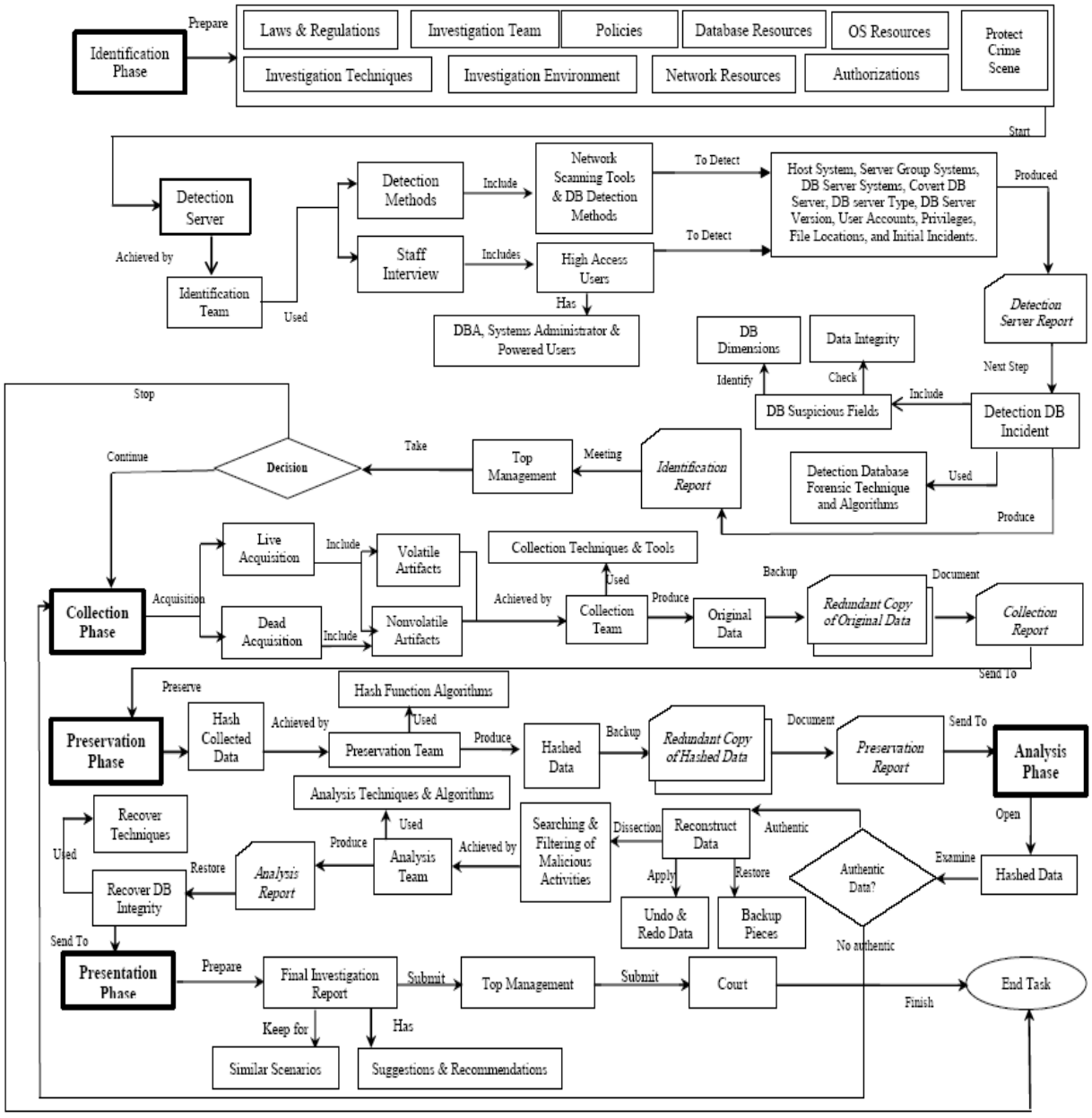

Fig. 2: Conceptual investigation process model for managing database forensic investigation knowledge

Table 2: Digital forensic process models

Model	Phases	Reference
M1	Aacquisition, Identification, Evaluation and Admission	Pollitt (1995)
M2	Acquiring, Authenticating and Analyzing the evidence	Kruse II and Heiser (2001)
M3	Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision	Palmer (2001)
M4	Identification, Preparation, Approach strategy, Preservation, Collection, Examination, Analysis, Presentation and Returning evidence	Reith *et al*. (2002)
M5	Readiness, Deployment, Physical crime scene investigation, Digital crime scene investigation and Review phases	Carrier and Spafford (2003)
M6	Readiness, Deployment, Traceback, Dynamite and Review.	Ciardhuáin (2004)
M7	Awareness, Authorization, Planning, Notification, Search for and identify evidence, Collection of evidence, Transport of evidence, Storage of evidence, Examination of Evidence, Hypothesis, Presentation of hypothesis, Proof/Defense of hypothesis and Archive storage	
M8	Preparation, Investigation and Presentation	Köhn *et al*. (2006)
M9	Pre-analysis, Analysis and Post-analysis phase	Freiling and Schwittay (2007)
M10	Planning, Identification, Reconnaissance, Transport and Storage, Analysis, Proof and Defense and Archive storage	Perumal (2009)
M11	Preparation, Incident, Incident response, Digital forensic investigation and Physical investigation and Presentation	Kohn *et al*. (2013)
M12	Suspend database operation, Collection, Preservation, Analysis, Reconstruct and Restore database integrity	Wong and Edwards (2004)
M13	Setting up the evidence collection server phase, Collecting an Oracle file of interest and Analysis phase	Tripathi and Meshram (2012)
M14	Investigation preparation, Incident verification, Artifact collection, Preservation, Artifact analysis and Report	Fowler (2008)

DATABASE FORENSIC INVESTIGATION CHALLENGES AND ISSUES

In fact, DBFI discipline is a young field which has been receiving a little of researches and attentions due to several challenges and issues.

The variety of database systems infrastructure such as an Oracle database, MS SQL server, MySQL database and DB2 has been producing complexity of database forensic investigation domain (Wong and Edwards, 2004), moreover the multidimensional nature of these systems has added more confusion in terms of forensic perspective, consequently, the diversity of database systems has been producing other challenge like different database artifacts (Ciardhuáin, 2004). Therefore, these challenges have been producing many issues like lack of perfect generic database forensic tool, detection method, collection method, or analyzing method. Other issues which have been producing owing to these challenges are scattered of DBFI knowledge anywhere in internet, books, books chapters, online database, experts, organizations and dissertation (Baker and Finkle, 2011). Therefore lack of obvious structure to managing and structuring this knowledge. Additionally, issues like rare of education, training, awareness, books and researches are other issues (Basu, 2006). Therefore this study provides survey of DBFI knowledge and proposed conceptual model which somehow is using to organizing and managing this knowledge.

CONCLUSION

Database forensic investigation discipline has been starving field owing to rare academic researches and attentions. Several database forensic investigation process models, detection and analysis algorithms and methods have been done, however most of them are scattered, specific and also lack of common investigation concepts and terminologies. Thus, this study proposed initial conceptual investigation process model through reviewed 14 digital investigation process models. The proposed model probably has covered most of the database forensic investigation knowledge concepts. On the other hand, challenges and issues which database forensic investigation community has been suffering are offered as well. The future work of this study will be validating and enhancing proposed conceptual model, thus details discussion of five proposed common investigation phases will be offered. Moreover, suggest metamodel for structuring and managing of database forensic investigation knowledge using metamodeling approach.

ACKNOWLEDGMENT

This research is supported by Universiti Teknologi Malaysia and MOHE through FRGS Grant No. R.J130000.7813.4F193.

REFERENCES

Al-Dhaqm, R., A. Mohammed, S.H. Othman, S. Abd Razak and A. Ngadi, 2014. Towards adapting metamodelling technique for database forensics investigation domain. Proceeding of the International Symposium on Biometrics and Security Technologies (ISBAST, 2014), pp: 322-327.

Azemović, J. and D. Mušić, 2009. Efficient model for detection data and data scheme tempering with purpose of valid forensic analysis. Proceeding of the 2009 International Conference on Computer Engineering and Applications (ICCEA, 2009).

Azemovic, J. and D. Music, 2010. Methods for efficient digital evidences collecting of business proceses and users activity in elearning enviroments. Proceeding of the International Conference on e-Education, e-Business, e-Management and e-Learning (IC4E'10), pp: 126-130.

Baker, L.B. and J. Finkle, 2011. Sony Playstation Suffers Massive Data Breach. Retreieved form: http://www.Reuters.com/article/us-sony-stoldendate-idUSTRE73P6WB20110426. (Accessed on: April 26, 2011)

Basu, A., 2006. Forensic Tamper Detection in SQL Server. Retrieved form: http://www.sqlsecurity.com/chipsblog/archivedposts.

Carrier, B. and E.H. Spafford, 2003. Getting physical with the digital investigation process. Int. J. Digit. Evidence, 2(2): 1-20.

Carvey, H., 2009. Windows Forensic Analysis DVD toolkit. 2nd Edn., Syngress, Burlington, MA.

Choi, J.H., D.W. Jeong and S. Lee, 2013. The method of recovery for deleted record in oracle database. J. Korea Inst. Inform. Secur. Cryptol., 23(5): 947-955.

Ciardhuáin, S.Ó., 2004. An extended model of cybercrime investigations. Int. J. Digital Evidence, 3(1): 1-22.

Clarke, J., 2012. SQL Injection Attacks and Defense. Elsevier Publisher, USA.

Cohen, F., 2012. Digital Forensic Evidence Examination. 4th Edn., ASP Press, New York.

Eessaar, E., 2006. Relational and Object-relational Database Management Systems as Platforms for Managing Software Engineering Artifacts. TUT Press, Tallinn.

Ericka, C., 2010. Ex-TSA Employee Indicted for Tempering with Database of Terrorist Suspects. Retrieved form: http://www.darkreading.com/database-security/167901020/security/applicationsecurity/223800029/ex-tsa-employee-indicted-for-tampering-with-database-ofterrorist-suspects.html. (Accessed on: Apr. 15, 2011)

Fasan, O.M. and M. Olivier, 2012. Reconstruction in database forensics. In: Peterson, G. and S. Shenoi (Eds.), Advances in Digital Forensics VIII, IFIP AICT 383, IFIP International Federation for Information Processing, pp: 273-287.

Fowler, K., 2008. SQL Server Forenisc Analysis. Pearson Education, ISBN: 0321617673, 9780321617675.

Freiling, F.C. and B. Schwittay, 2007. A common process model for incident response and computer forensics. IMF, 7: 19-40.

Fruhwirt, P., M. Huber, M. Mulazzani and E.R. Weippl, 2010. Innodb database forensics. Proceeding of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA, 2010), pp: 1028-1036.

Fruhwirt, P., P. Kieseberg, S. Schrittwieser, M. Huber and E. Weippl, 2012. InnoDB database forensics: reconstructing data manipulation queries from redo logs. Proceeding of the 7th International Conference on Availability, Reliability and Security (ARES, 2012), pp: 625-633.

Frühwirt, P., P. Kieseberg, S. Schrittwieser, M. Huber and E. Weippl, 2013. InnoDB database forensics: Enhanced reconstruction of data manipulation queries from redo logs. Inform. Secur. Technical Report, 17(4): 227-238 .

Guimaraes, M.A., R. Austin and H. Said, 2010. Database forensics. Proceeding of the 2010 Information Security Curriculum Development Conference, pp: 62-65.

Haerder, T. and A. Reuter, 1983. Principles of transaction-oriented database recovery. ACM Comput. Surv. (CSUR), 15(4): 287-317.

Jin, X. and S.L. Osborn, 2007. Architecture for Data Collection in Database Intrusion Detection Systems. In: Secure Data Managemeny, Springer, Berlin, Heidelberg, pp: 96-107.

Kambire, M.K., P.H. Gaikwad, S.Y. Gadilkar and Y.A. Funde, 2015. An improved framework for tamper detection in databases. Int. J. Comput. Sci. Inform. Technol., 6(1): 57-60.

Kaplan, D., 2012. Hackers Breach Environment Protection Agency Database. Retrieved Nov, 20, 2012.

Khanuja, H.K. and D.D. Adane, 2012. A framework for database forensic analysis. Published Comput. Sci. Eng. Int. J., 2(3).

Köhn, M., M.S. Olivier and J.H. Eloff, 2006. Framework for a digital forensic investigation. Proceeding of the 2006 ISSA, pp: 1-7.

Kohn, M.D., M.M. Eloff and J.H. Eloff, 2013. Integrated digital forensic process model. Comput. Secur., 38: 103-115.

Kruse II, W.G. and J.G. Heiser, 2001. Computer Forensics: Incident Response Essentials. Pearson Education.

Lee, G.T., S. Lee, E. Tsomko and S. Lee, 2007. Discovering methodology and scenario to detect covert database system. Proceeding of the 2007 Future Generation Communication and Networking (FGCN, 2007), pp: 130-135.

Lee, K.G., A. Savoldi, P. Gubian, K.S. Lim, S. Lee and S. Lee, 2008. Methodologies for detecting covert database. Proceeding of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP'08), pp: 538-541.

Litchfield, D., 2007a. Oracle Forensics Part 1: Dissecting the Redo Logs. NGSSoftware Insight Security Research (NISR) Publication, Next Generation Security Software Ltd., Sutton.

Litchfield, D., 2007b. Oracle forensics Part 2: Locating Dropped Objects. NGSSoftware Insight Security Research (NISR) Publication, Next Generation Security Software. (Retrieved from: http://www.davidlitchfield.com/.)

Litchfield, D., 2007c. Oracle Forensics: Part 3 Isolating Evidence of Attacks Against the Authentication Mechanism. NGSSoftware Insight Security Research (NISR).

Litchfield, D., 2007d. Oracle forensics Part 4: Live Response. NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd., Sutton.

Litchfield, D., 2007e. Oracle Forensics Part 5: Finding Evidence of Data Theft in the Absence of Auditing. NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd., Sutton.

Litchfield, D., 2007f. Oracle Forensics Part 6: Examining Undo Segments, Flashback and the Oracle Recycle Bin. NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd., Sutton.

Litchfield, D., 2008. Oracle Forensics Part 7: Using the Oracle System Change Number in Forensic Investigations. NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd., Sutton.

Litchfield, D., C. Anley, J. Heasman and B. Grindlay, 2005. The Database Hacker's Handbook: Defending Database Servers. Wiley, New York.

Montalbano, E., 2011. Anonymous Claims Hack on NATO Servers: Retrieved Sep.

Natan, R.B., 2005. Implementing Database Security and Auditing. Digital Press.

Ngadi, M., R. Al-dhaqm and A. Mohammed, 2012. Detection and prevention of malicious activities on RDBMS relational database management systems. Int. J. Sci. Eng. Res., 3(9): 1-10.

Olivier, M.S., 2009. On metadata context in database forensics. Digit. Invest., 5(3): 115-123.

Palmer, G., 2001. A road map for digital forensic research. Proceeding of the 1st Digital Forensic Research Workshop. Utica, New York, pp: 27-30.

Pavlou, K.E. and R.T. Snodgrass, 2008. Forensic analysis of database tampering. ACM T. Database Syst., pp: 1-45.

Pavlou, K.E. and R.T. Snodgrass, 2010. The tiled bitmap forensic analysis algorithm. IEEE T. Knowl. Data En., 22(4): 590-601.

Perumal, S., 2009. Digital forensic model based on Malaysian investigation process. Int. J. Comput. Sci. Network Secur., 9(8): 38-44.

Pollitt, M., 1995. Computer forensics: An approach to evidence in cyberspace. Proceeding of the National Information Systems Security Conference, pp: 487-491.

Qian, L., H. Xueli and W. Hao, 2014. Database management strategy and recovery methods of android. Proceeding of the 5th IEEE International Conference on Software Engineering and Service Science (ICSESS, 2014), pp: 727-730.

Reith, M., C. Carr and G. Gunsch, 2002. An examination of digital forensic models. Int. J. Digit. Evidence, 1(3): 1-12.

Shearer, L., 2012. UGA says digital intruders got personnel record access. Retrieved Nov. 20, 2012.

Snodgrass, R.T., S.S. Yao and C. Collberg, 2004. Tamper detection in audit logs. Proceeding of the 13th International Conference on Very Large Data Bases, 30: 504-515.

Son, N., K.G. Lee, S. Jeon, H. Chung, S. Lee and C. Lee, 2011. The method of database server detection and investigation in the enterprise environment. In: Park, J.J. (Eds.), STA, 2011. CCIS 186, Springer-Verlag, Berlin, Heidelberg, pp: 164-171.

Spreitzenbarth, M., S. Schmitt and F. Freiling, 2012. Comparing sources of location data from android smartphones. In: Peterson, G. and S. Shenoi (Eds.), Advances in Digital Forensics VIII, IFIP Advances in Information and Communication Technology. Springer, Berlin, Heidelberg, pp: 143-157.

Suffern, L., 2010. A study of current trends in database forensics. J. Dig. Forensic Practice, 3(2-4): 67-73.

Tripathi, S. and B.B. Meshram, 2012. Digital evidence for database tamper detection. J. Inform. Secur., 3: 113-121.

Williams III, R.H., 2006. Introduction to Information Security Concepts.

Wong, D. and K. Edwards, 2004. System and Method for Investigating a Data Operation Performed on a Database. Publication number US20050289187 A1.

Wright, P.M., 2005. Oracle database forensics using logminer option 3-perform forensic tool validation. Proceeding of the GCFA Assignment-GSEC, GCFW and GCIH, London.

Wright, P.M. and D. Burleson, 2008. Oracle Forensics: Oracle Security Best Practices. Rampant Tech Press.

Wu, B., M. Xu, H. Zhang, J. Xu, Y. Ren and N. Zheng, 2013. A recovery approach for SQLite history recorders from YAFFS2. Proceeding of Information and Communication Technology-EurAsia Conference. Yogyakarta, Indonesia, pp: 295-299.

Xu, M., X., Yang, B., Wu, J., Yao, H., Zhang and J. Xu, 2013. A metadata-based method for recovering files and file traces from YAFFS2. Digit. Invest., 10(1): 62-72.