SIMPLIFIED DATABASE FORENSIC INVETIGATION USING METAMODELING APPROACH

ARAFAT MOHAMMED RASHAD AL-DHAQM

A thesis submitted in partial fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

FEBRUARY 2019

DEDICATION

To my parents, Mohammed Rashad Aldoqm and Safia Ali Aldoqm, for their endless love, support and whose good examples have taught me to work hard for the things that I aspire to achieve. Also, to my wife, Safa Ahmed Ali Aldoqm and my daughter, Hadeel Arafat for their words of encouragement to keep on striving to complete this study. Likewise, to my uncle, Dr.Ahmed Ali Aldoqm for his encouragement and supporting to complete this study. And finally, to my brothers, and sisters, Hammeed, Abdualwahead, Jamelh, Arwa, Noha, Najat, and Ebtisam for their supporting.

ACKNOWLEDGEMENT

First and foremost, I will like to thank the Almighty Allah Subhanaha wa ta'ala for giving me the strength, wisdom and guidance to produce this work. May the peace and blessings of Allah be upon his noble prophet Muhammad (SWA), his family and companions. Next, I wish to thank Universiti Teknologi Malaysia for giving the enabling environment and publication support. I feel highly indebted to my supervisors Associate Professor Dr. Shukor Abd Razaq, Dr. Siti Hajar Othman and Associate Professor Dr. Md Asri Ngadi for their guidance, encouragement, support, criticism and very useful suggestions throughout the PhD programme and the thesis preparation. Also, I would like to thank Professor John Walker, Associate Professor Dr. Siti Rahayu Selamat, Expert Mahesa Sankarra, Expert Daniele, and Digital Forensic Experts in at Cybersecurity Malaysia for their time and efforts to evaluate this study.

ABSTRACT

Database Forensic Investigation (DBFI) domain is a significant field used to identify, collect, preserve, reconstruct, analyze and document database incidents. However, it is a heterogeneous, complex, and ambiguous domain due to the variety and multidimensional nature of database systems. Numerous specific DBFI models and frameworks have been proposed to solve specific database scenarios but there is a lack of structured and unified frameworks to facilitate managing, sharing and reusing of DBFI tasks and activities. Thus, this research developed a DBFI Metamodel (DBFIM) to structure and organize DBFI domain. A Design Science Research Methodology (DSRM) to provide a logical, testable and communicable metamodel was applied in this study. In this methodology, the steps included problem identification, define objectives, design and development, demonstration and evaluation, and communication. The outcome of this study is a DBFIM developed for structuring and organizing DBFI domain knowledge that facilitates the managing, sharing and reusing of DBFI domain knowledge among domain practitioners. DBFIM identifies, recognizes, extracts and matches different DBFI processes, concepts, activities, and tasks from different DBFI models into a developed metamodel, thus, allowing domain practitioners to derive/instantiate solution models easily. The DBFIM was validated using qualitative techniques: comparison against other models; face validity (domain experts); and case study. Comparisons against other models and face validity were applied to ensure completeness, logicalness, and usefulness of DBFIM against other DBFI domain models. Following this, two case studies were selected and implemented to demonstrate the applicability and effectiveness of the DBFIM in the DBFI domain using a DBFIM Prototype (DBFIMP). The results showed that DBFIMP allowed domain practitioners to create their solution models easily based on their requirements.

ABSTRAK

Domain Siasatan Forensik Pangkalan Data (DBFI) merupakan satu bidang penting untuk mengenal pasti, mengumpul, memelihara, membina semula, menganalisis dan mendokumenkan insiden pangkalan data. Walau bagaimanapun, ia merupakan domain yang heterogen, kompleks dan taksa disebabkan sifat kepelbagaian dan berbilang dimensi sistem pangkalan data. Banyak model dan rangka kerja DBFI khusus telah dicadangkan untuk menyelesaikan senario khusus pangkalan data tetapi masih kurang rangka kerja yang berstruktur dan bersepadu bagi memudahkan pengurusan, perkongsian dan penggunaan semula tugas dan aktiviti DBFI. Oleh itu, penyelidikan ini telah membangunkan satu Metamodel DBFI (DBFIM) untuk menstruktur dan menyusun domain DBFI. Kaedah Penyelidikan Sains Reka Bentuk (DSRM) untuk menyediakan metamodel yang logik, boleh diuji dan dapat berkomunikasi digunakan dalam kajian ini. Dalam kaedah ini, langkah-langkah adalah termasuk pengenalpastian masalah, penentuan objektif, reka bentuk dan pembangunan, demonstrasi dan penilaian serta komunikasi. Hasil kajian ini ialah satu DBFIM dibangunkan untuk menstruktur dan menyusun ilmu domain DBFI yang memudahkan pengurusan, perkongsian dan penggunaan semula ilmu domain DBFI dalam kalangan pengamal domain. DBFIM mengenal pasti, mengecam, mengekstrak dan memadankan proses, konsep, aktiviti dan tugas DBFI yang berbeza daripada model DBFI yang berlainan menjadi metamodel maju, lantas membolehkan pengamal domain untuk menerbitkan model penyelesaian dengan mudah. DBFIM disahkan menggunakan teknik kualitatif: perbandingan terhadap model-model lain; kesahan muka (pakar domain); dan kajian kes. Perbandingan terhadap model-model lain dan kesahan muka digunakan untuk memastikan kesempurnaan, kelogikan dan kebergunaan DBFIM berbanding model-model domain DBFI lain. Berikutan ini, dua kajian kes dipilih dan dilaksanakan untuk menunjukkan kebolehgunaan dan keberkesanan DBFIM dalam domain DBFI menggunakan Prototaip DBFIM (DBFIMP). Keputusan menunjukkan bahawa DBFIM membolehkan pengamal domain untuk mencipta model penyelesaian mereka dengan mudah berdasarkan keperluan mereka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DBFI	-	Database Forensic Investigation
DBFIM	-	Database Forensic Investigation Metamodel
DBMS	-	Database Management System
RDBMS	-	Relational Database Management System
MSSQL	-	Microsoft Structure Query Language
MDE	-	Model Driven Architecture
DSRM		Design Science Research Methodology
DBFIMP	-	Database Forensic Investigation Metamodel Prototype
DML	-	Data Manipulation Language
DDL	-	Data Definition Language
SQL	-	Structured Query Language
RGB	-	Red Green Blue
RGBY	-	Red Green Blue Yellow
GUAM	-	Generalized Update Access Method
NAA	-	North American Aviation
IBM	-	International Business Machine
CODASYL	-	Committee on Data Systems Languages
ANSI	-	American National Standards Institute's
SPARC	-	Standards Planning and Requirements Committee
WAL	-	Write-ahead logging
SMS	-	Short Message Service
DFs	-	Digital Forensics
QVT	-	Query/Views/Transformation
UML	-	Unified Modeling Language
OMG	-	Object Management Group
DBFI	-	Database Forensic Investigation
DBFIM	-	Database Forensic Investigation Metamodel
DBMS	-	Database Management System
RDBMS	-	Relational Database Management System
MSSQL	-	Microsoft Structure Query Language

MDE	-	Model Driven Architecture
DSRM		Design Science Research Methodology
DBFIMP	-	Database Forensic Investigation Metamodel Prototype

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Database Forensic Investigation (DBFI) is a branch of Digital Forensics (DFs) that examines database content to confirm database crimes. It is considered a significant field by which to identify, detect, acquire, analyse, and reconstruct database incidents and reveal intruders' activities. DBFI domain has suffered from several issues, which has resulted in it becoming a heterogeneous, confusing and unstructured domain. Examples of these issues include a variety of database system infrastructures; the multidimensional nature of database systems; and domain knowledge effectively being scattered in all directions. A variety of database system infrastructures with multidimensional natures has enabled the DBF domain to address specific incidents. Therefore, each database management system (DBMS) has a specific forensic investigation model/approach. Consequently, the issues of different concepts and terminologies in terms of the forensic investigation process and the scattering of domain knowledge in all directions have produced other challenges for DBF investigators and practitioners. This knowledge (such as models, processes, techniques, tools, frameworks, methods, activities, approaches, and algorithms) is neither organized nor structured. Furthermore, it is universally dispersed, such as in the Internet, books, journals, conferences, online databases, book chapters, dissertations, reports, and organizations. Consequently, there is a lack of generic/standardized models by which to unify concepts and terminologies that may be used to reduce confusion and assist in organizing and structuring domain knowledge.

This chapter summarizes a background of the research problem which ends with formulating the problem statement. The problem statement is broken down into a main research question with four sub-questions. To answer the research questions,

this research targets three objectives to be accomplished through this research. This chapter also identifies the scope within which the research will be covered. It also illustrates the significance of the research and provides contributions of the research as well as describing the outline of the study.

1.2 Background of the Problem

DBFI domain is dealing with database content and their metadata (data dictionary) to identify, collect, preserve, reconstruct, analyze and document evidences against database incidents (Olivier, 2009). However, few researchers were carried out and it received little attention due to the complexity and multidimensionality of Database Management Systems (DBMSs) (Adedayo and Olivier, 2015; Beyers, 2014; Fowler, 2008; Khanuja and Adane, 2012b; Olivier, 2009; Wagner *et al.*, 2015). Therefore, there are limited practical researches concerning DBFI domains to solve specific issues. The specific practical DBFI researches covered various DBMSs as shown in Figure 1.1.

Specific and limited Oracle database investigation models, processes, concepts, tasks, activities, and techniques have been proposed in the literature (Litchfield, 2007a; 2007b; 2007c; 2007d; 2007e; 2007f; 2008; Tripathi and Meshram, 2012; Wong and Edwards, 2004; Wright, 2005). For example, the forensic investigation model has been proposed by Wong and Edwards (2004) that consists of specific steps to discover information about an operation performed on a database (Olivier, 2009). Also, the Log Miner tool has been proposed by Wright (2005) that allows a DBA or forensic analyst to reconstruct actions that took place on a database (Fasan and Olivier, 2012a). Moreover, seven (7) practical investigation forensic models have been proposed by Litchfield (2007) that addressed information available from redo logs, dropped objects, authentication, flashback, and recycle bin. Forensic text book has been published on Oracle database by Wright and Burleson (2008), however the book is written at a practical level and intended for database administrators (Olivier, 2009). Also, the investigation model to collect evidences from

compromised database was introduced by Tripathi and Meshram (2012) based on a series of practical methods that proposed by Litchfield (2007).

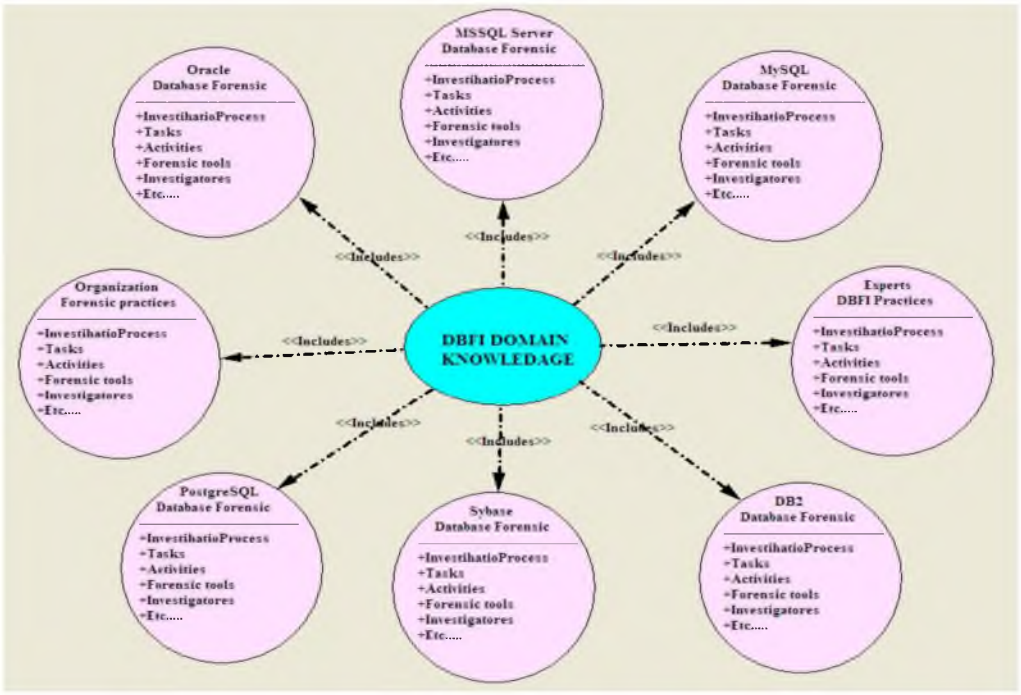

Figure 1.1 Practical DBFI researches that covered various DBMSs

Similarly, the Microsoft SQL (MSSQL) database has limited and specific forensic practical researches that are proposed in the literature (Basu, 2006; Fowler, 2008; Fowler *et al.*, 2007; Khanuja and Adane, 2013; Son *et al.*, 2011). For example SQL Server Forensic Analysis Methodology proposed by Fowler (2008) and consists of four investigation phases namely investigation preparation, incident verification, artifact collection, and artifact analysis which deal with the MSSQL server database (Fasan and Olivier, 2012a; Wagner *et al.*, 2015). A practical real world scenario has been proposed by Fowler *et al.* (2007) to gather and analyze all evidences from a compromised database. It covers technical concepts that investigators need when a database becomes compromised or changed. A model of forensic tamper detection of sensitive data has been proposed by Basu (2006) to detect database tampering. A detection and investigation model has been developed by Son *et al.* (2011) to detect database server, collect data and investigate data collected. Another methodology has

been proposed by Khanuja and Adane (2013) to detect suspicious transactions within a database.

Additionally, MySQL RDBMS has limited and specific forensic practical researches that are proposed in the literature (Fruhwirt *et al.*, 2010; Frühwirt *et al.*, 2012; 2013; Khanuja and Adane, 2012b; Lawrence, 2014; OGUTU, 2016). For example, a framework for MySQL database forensic analysis has been proposed by Khanuja and Adane (2012) which concentrated on discovering malicious tampering in MySQL database. Also a MySQL database detection inconsistencies model has been proposed by Fruhwirt *et al.* (2010) to identify and detect conflicts in database records. A reconstructing basic SQL statements model has been proposed by Fruhwirt *et al.* (2012) to reconstruct basic SQL statements from InnoDB's redo logs. However, it concentrated on Data Manipulation Language (DML) statements and ignored Data Definition Language (DDL) statements (Frühwirt *et al.*, 2013). Improvements have been made to enhance the previous reconstructing model by Fruhwirt *et al.* (2013) that includes reconstructing DDL statements. Additionally, a technical investigation model proposed by Lawrence (2014) to get admission to a user's MySQL database without the need for the user's assistance. This is beneficial in cases of emergency where the user is absent or where the user is under examination. Forensic investigation methodology has been proposed by OGUTU (2016) for testing the forensic richness of a storage engine of the MySQL database system. It consists of three investigation processes which are Preliminary analysis, Execution, and Analysis process to investigate the impact of storage engines in the generation of persistent forensic data in MySQL DBMS system.

Apart from various DBFI domain knowledge proposed for DBMS, there are also several forensic tamper detection models and analysis algorithms of database systems proposed in the literature (Adedayo, 2015; Beyers *et al.*, 2014; Khanuja and Suratkar, 2014; Pavlou and Snodgrass, 2008; 2010; 2013; Snodgrass *et al.*, 2004; Wagner *et al.*, 2015; Wagner *et al.*, 2017). For example, tampering on database can be detected and analyzed by using various forensic algorithms proposed by (Pavlou and Snodgrass, 2008; 2013; Snodgrass *et al.*, 2004). A model to investigate a compromised database management system has been proposed by Beyers (2014) (Beyers, 2014)

(Beyers, 2014) (Beyers, 2014) (Beyers, 2014) (Beyers, 2014) (Beyers, 2014) (Beyers, 2014) (Beyers, 2014) (Beyers, 2014) (Beyers, 2014). It contains of two investigation processes namley identification and collection. The identification process is intended to prepare database forensic layers, methods and environment, while the collection process permits one to gather doubted database management system data and move it to a protected area for further forensic examination. A model to collect, preserve and analyze database metadata against database attacks has been proposed by Khanuja and Suratkar (2014). It proposed four main investigation processes which are *collection and preservation, analysis of anti-forensic attacks, analysis database attack, and preserving evidence report*. Additionally, a model proposed by Frühwirt *et al.* (2014) to reconstruct database events to detect intruder activities, via two investigation process which are *a collection process and* a *reconstructing evidence process.* An investigation process model has been proposed by Adedayo and Olivier (2015) to reconstruct and analyze database activity using log files via two processes which are *the reconstruction process and analysis process*. Finally, Wagner *et al.* (2017) presented reconstruction model for rebuilding database content from a database image without using any log or system metadata. A special forensic tool called "*DBCarver*" has been presented for this task that permits reconstruction of database storage.

Therefore, various DBFI models, frameworks, processes, concepts, activities, tasks, and techniques have been proposed which resulted of redundancy of investigation processes, concepts, activities, and tasks. Existing researches discussed DBFI domain from three perspectives: technology perspective (tools, algorithms, and methods), investigation process perspective (identification, collection, preservation, examination, analysis, reconstruction, presentation) and dimension perspective (destroyed dimension, compromised dimension, changed dimension) (Fasan and Olivier, 2012a). Consequently, DBFI domain lack of structured and unified model to facilitates in managing, sharing, and reusing DBFI domain knowledge amongst domain practitioners (Adedayo, 2015; Beyers, 2014; Fasan and Olivier, 2012a; Hauger and Olivier, 2015). The motivation of this study is to develop a unified and structured a metamodel to facilitate the needs, report, or data shares that are important to the domain practitioners.

Additionally, the primary study (interview) which was conducted with domain experts showed the DBFI domain needs standard guideline/process flow to conduct database forensic investigation. For example, the CyberSecurity domain experts stated: "In most cases we need to have an overall view of database forensic investigation process. A comprehensive one is helpful and better for better understanding. Thus, we need a standard guideline/process flow to conduct database forensic investigation". Also, Professor John Walker stated: "As Digital Forensics requires a robust set of processes and procedures to support the activity, it follows that when a First Responder or Investigator engages an incident which includes a database (of whatever form), and such a process would prove an asset to underpin such an activity. Thus, it is important to have documented, robust directives which can accommodate the dissemination of valuable knowledge, and to provision a consistent process to enable such investigations". Appendix A displays expert's interview of DBFI domain requirements.

Therefore, and based on the primary and secondary studies, the DBFI domain lacks a comprehensive model/framework to guides domain practitioners to conduct database forensic investigation easily. Figure 1.2 summarizes the research background of this study which leads to the formulation of the problem statement.

1.3 Problem Statement

Based on the primary and secondary studies that discussed in Section 1.2, the DBFI is a heterogeneous, complex and ambiguous domain. It receives little attention amongst researchers due to the diversity and multidimensionality of database systems(Adedayo, 2015; Fasan and Olivier, 2012a; Guimaraes *et al.*, 2010; Khanuja and Adane, 2012b; Olivier, 2009; Yoon *et al.*, 2016)(Adedayo, 2015; Fasan and Olivier, 2012a; Guimaraes *et al.*, 2010; Khanuja and Adane, 2012b; Olivier, 2009; Yoon *et al.*, 2016). Current researches have not focused on fundamental and essential guidelines for establishing a baseline for DBFI domain, but focused instead on specific procedures and principles of technical issues in solving specific problems(Beyers, 2014; Fasan and Olivier, 2012a; Olivier, 2009; Yoon *et al.*, 2016)(Beyers, 2014; Fasan

and Olivier, 2012a; Olivier, 2009; Yoon *et al.*, 2016). Therefore, there is a lack of structured and unified models to facilitate the needs, report, or data shares that is important to the domain practitioners.

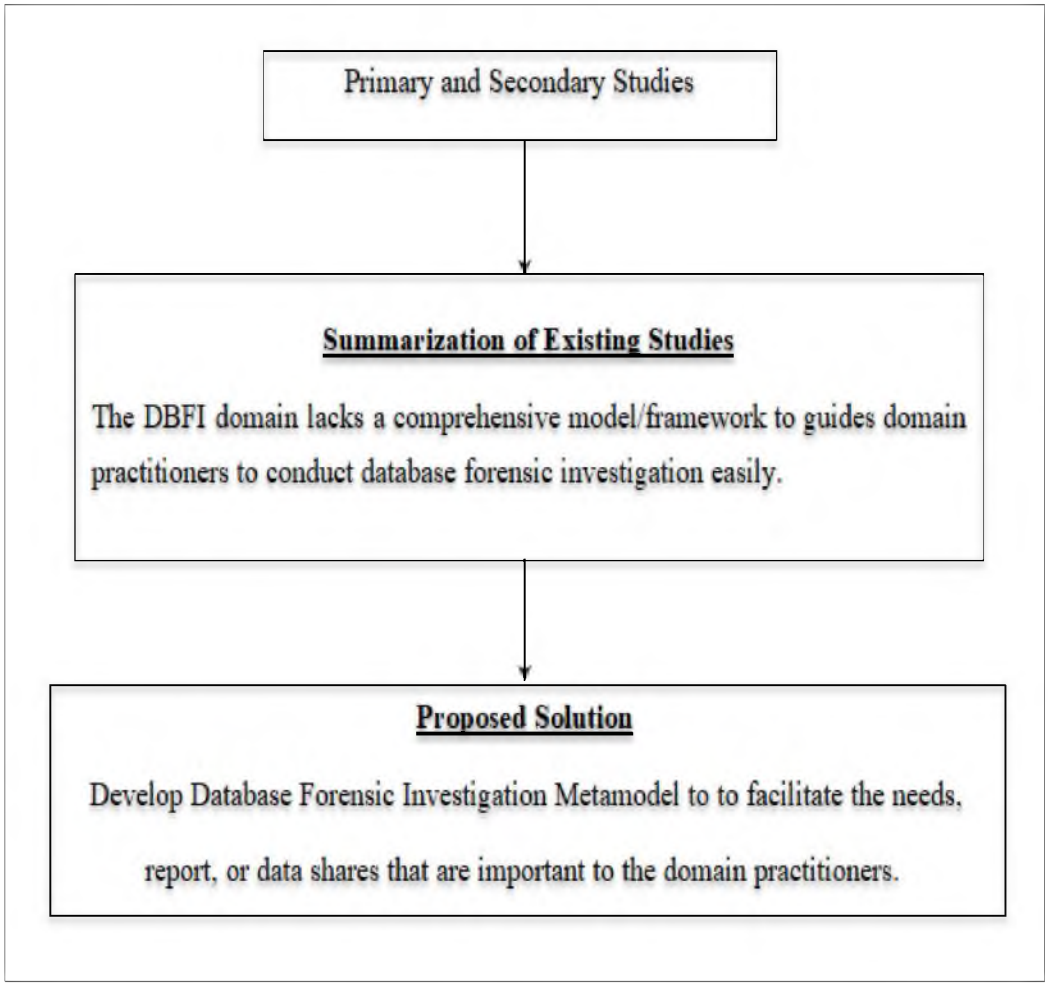

Figure 1.2 Summary of Research Background

1.4 Research Questions

Based on the discussion in the previous section, the research problem is broken down into research questions:

i. What are the common DBFI concepts and processes?

ii. How to develop and validate a metamodel for DBFI knowledge domain?

iii. How can demonstrate and evaluate the DBFIM?

1.5 Research Objectives

To answer research questions, this research targets accomplishing the following research objectives:

i. To propose common investigation processes and concepts for the DBFI domain to solve the issue of redundancy of processes and concepts of the DBFI domain.

ii. To develop and validate a Database Forensic Investigation Metamodel (DBFIM).

iii. To demonstrate and evaluate the effectiveness and applicability of the DBFIM in the real scenarios of DBFI domain.

1.6 Research Scope

The study is limited to the Relational Database Management Systems (Oracle RDBMS, MSSQL RDBMS, MySQL RDBMS, SQLite RDBMS, DB2 RDBMS, and Sybase RDBMS).

1.7 Research Significance

This study is vital and meaningful from theoretical/conceptual points of view. Thus, metamodeling approaches are useful for modeling such heterogeneous, complex, and ambiguous domains to produce metamodeling language called metamodel. Metamodel facilitates in managing, sharing and reusing such domain

knowledge. DBFI domain is a heterogeneous, complex and ambiguous domain. Therefore, research in this area is significant, since it will shed light on the importance and affects the metamodeling approach on DBFI domain. The outcomes of this study are believed to be useful to DBFI domain practitioners. The proposed metamodel will be used to solve database incidents by developing specific solution models from the proposed DBFIM. Furthermore, it will be used by domain practitioners as a guideline. This study is significant and helpful for the laboratory to understand better about process involves in the DBFI domain. It contains main concepts of DBFI domain in a single model; therefore, facilitate fast understanding. Certainly, it's beneficial for the digital forensic laboratory. This model is useful for domain practitioners (incident responders, examiners, investigators, and analysers) to explain the concepts of DBFI to newly employed staff, as well as to the investigation team.

1.8 Research Contributions

This study contributes to the solution of the interoperability, heterogeneity, and complexity issues of the DBFI domain through the proposal of a new structured and unified metamodel (DBFIM) which facilitates in managing, sharing and reusing DBFI domain knowledge. This is an explicit artefact to describe whole DBFI knowledge. After the research follow completed and explaining DBFIM benefits from expert's perspective, the findings of this research can not only assist domain practitioners (incident responders, examiners, investigators, and analysers) in the development of solution models for their problems, but can also provide insight into how to promote the newcomers to use this metamodel as a guideline to investigate database incidents. The benefits of the DBFIM to the domain practitioners are:

i. Simplify common communication amongst different DBFI domain practitioners through a common representation layer that includes all the processes, concepts, tasks and activities that must exit in DBFI domain.

ii. Provide guidelines and new model developing process that assists domain practitioners in managing, sharing and reusing DBFI domain knowledge.

iii. Enable domain practitioners to create a new solution model easily through electing and combining sets of concept elements (attribute and operations) based on their own model requirement.

iv. Enable domain practitioners to gain quick access to previous relevant DBFI domain knowledge and allow them to reuse this knowledge.

1.9 Thesis Structure

This study consists of seven chapters as follows:

Chapter 1 discusses the problem background, problem statement, research questions, research objectives, contribution, research significance, scope of the study and describes the outline of the study.

Chapter 2 discusses the review of the literature of the study area. It highlights two main concepts. It concentrates on DBFI, and Model Driven Engineering (MDE). It begins by introducing the DBFI knowledge domain which includes models, frameworks, approaches, methods, activities, tasks, concepts, practitioners, and processes, as well as addressing the main gap of the DBFI. Also, it introduces the MDE concepts that include models, metamodels, metamodel transformation, metamodeling frameworks, and metamodeling development processes. Additionally, this chapter introduces the validation techniques which will be used during this study.

Chapter 3 provides the research methodology of this study. It contains the general framework of the research as well as the steps required to carry out the research systematically. It introduces the Design Science Research Methodology (DSRM) that is used in this study.

Chapter 4 addresses the first and second objectives of the research. This chapter proposes a common investigation processes and concepts for DBFI domain. Nineteen (19) DBFI models have been identified and selected from a literature review to propose common DBFI processes and concepts. Then, four (4) common investigation processes have been proposed for DBFI domain based on their frequency and

appearances amongst models: *Identification process, Artifact Collection, Artifact Analysis, and Documentation and Presentation process*. Also, it offers validation technique that is used to validate the completeness and coherence of proposed common investigation process: comparison against other models. Also, this chapter proposes common concepts and terminologies of the DBFI domain. Therefore, this study identifies, recognizes, extracts, nominates and proposes the common concepts and terminologies. The concepts which have a similar meaning (semantically) or functioning, along with different names, or synonyms should be gathered and unified in one concept.

Chapter 5 discusses the development and validation of the Database Forensic Investigation Metamodel (DBFIM). This is the third objective of the research. The common processes and concepts that were proposed in Chapters 4 are used as bases for the development of the DBFIM. The first version of the proposed DBFIM is also presented. It also presents validation of the proposed DBFIM. Two validation techniques are presented in this chapter namely "*Comparison against other models*", and "*Face-Validity*" to validate the completeness, usefulness, and logicalness of the DBFIM.

Chapter 6 evaluates the proposed DBFIM through the development of a prototype. The prototype consists of three main components: DBFIM components, DBFIM knowledge base and DBFIM Modeling units. It also, evaluates the conducted case studies.

Chapter 7 concludes this study by presenting the summary of all research activities discussed in this study. The chapter contains brief discussions about the proposed process, concepts, DBFIM, research contributions and future work.

REFERENCES

Abdullah, A., Othman, S. H. and Razali, M. N. (2006). Structuring Knowledge on House Price Volatility Through A metamodel. *ARPN Journal of Engineering and Applied Sciences*, 10(23), 17785-17795.

Adedayo, O. M. (2015). Reconstruction in Database Forensics. *Doctoral dissertation, University of Pretoria.*

Adedayo, O. M. and Olivier, M. S. (2015). Ideal Log Setting for Database Forensics Reconstruction. *Digital Investigation*, 12, 27-40.

Ahmad, M. N., Colomb, R. M. and Sadiq, S. W. (2010). A UML Profile for Perdurant Ontology of Domain Interlocking Institutional Worlds. *International Journal of Internet and Enterprise Management*, 6(3), 213-232.

Akinyemi, J. A., Clarke, C. L. and Kolla, M. (2010). Towards A Collection-Based Results Diversification. Proceedings of the 2010 *Adaptivity, Personalization and Fusion of Heterogeneous Information*, 202-205.

Al-Rubaiy, H. M. M. (2014). *Query processing for data retrieval from distributed database management system.* Eastern Mediterranean University (EMU)-Doğu Akdeniz Üniversitesi (DAÜ).

Ali, A., Razak, S. A., Othman, S. H., Mohammed, A. and Saeed, F. (2017). A Metamodel for Mobile Forensics Investigation Domain. *PloS one*, 12(4), e0176223.

Archer, B., and Cross, N. (1984). Developments in design methodology (pp. 202-220): Chichester: Wiley.

Aßmann, U., Zschaler, S. and Wagner, G. (2006). Ontologies, Meta-models, and the Model-driven Paradigm *Ontologies for Software Engineering and Software Technology* (pp. 249-273): Springer.

Atkinson, C. and Kuhne, T. (2003). Model-driven Development: A Metamodeling Foundation. *IEEE Software*, 20(5), 36-41.

Authosserre-Cavarero, A., Bertrand, F., Blay-Fornarino, M., Collet, P., Dubois, H., Ducasse, S., et al. (2012). Interopérabilité des Systèmes D'information: Approches Dirigées Par les Modèles. Proceedings of the 2012 *Inforsid 2012*, 11-30.

Azemovic, J. and Music, D. (2010). Methods for Efficient Digital Evidences Collecting of Business Proceses and Users Activity in eLearning Enviroments. Proceedings of the 2010 *e-Education, e-Business, e-Management, and e-Learning, 2010. IC4E'10. International Conference on*, 126-130.

zemović, J., and Mušić, D. (2009). *Efficient model for detection data and data scheme tempering with purpose of valid forensic analysis.* Paper presented at the 2009 International Conference on Computer Engineering and Applications (ICCEA 2009), 83-89.

Banciihon, F. (1988). Object-Oriented Database Systems. Proceedings of the 1988 *Proceedings of the Seventh ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, 152-162.

Bandara, W., Indulska, M., Chong, S. and Sadiq, S. (2007). Major Issues in Business Process Management: An Expert Perspective, In Proceedings ECIS 2007 - The 15th European Conference on Information Systems, 1240-1251.

Bassil, Y. (2012). A comparative study on the performance of the Top DBMS systems. *arXiv preprint arXiv:1205.2889*, 20-31.

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

Bermell-Garcia, P. (2007). A metamodel to annotate knowledge based engineering codes as enterprise knowledge resources, *Phd Thesis, School of Applied Sciences, Cranfield University.*

Beydoun, G., Low, G., Henderson-Sellers, B., Mouraditis, H., Sanz, J. J. G., Pavon, J., et al. (2009). FAML: A Generic Metamodel for MAS Development. *IEEE Transactions on Software Engineering*, 35(6), 841-863.

Beyers, H., Olivier, M. and Hancke, G. (2011). Assembling metadata for database forensics *Advances in Digital Forensics VII* (pp. 89-99): Springer.

Beyers, H., Olivier, M. S. and Hancke, G. P. (2012). Arguments and Methods for Database Data Model Forensics. Proceedings of the 2012 *WDFIA*, 139-149.

Beyers, H. Q. (2014). Database forensics: Investigating compromised database management systems. PhD dissertation, University of Pretoria.

Beyers, H. Q., Oliviery, M. S. and Hancke, G. P. (2014). Database application schema forensics. *South African Computer Journal*, 55, 1-11.

Bézivin, J. and Gerbé, O. (2001). Towards a precise definition of the OMG/MDA framework. Proceedings of the 2001 *Automated Software Engineering,*

2001.(ASE 2001). Proceedings. 16th Annual International Conference on, 273-280.

Bogen, A. C. (2006). *Selecting keyword search terms in computer forensics examinations using domain analysis and modeling*: Mississippi State University.

Bogen, A. C. and Dampier, D. A. (2005). Unifying computer forensics modeling approaches: a software engineering perspective. Proceedings of the 2005 *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, 27-39.

Bosworth, S. and Kabay, M. E. (2002). *Computer security handbook*: John Wiley & Sons.

Buang, M. F. M. and Daud, S. M. (2012). A web-based KM system for digital forensics-knowledge sharing capability. Proceedings of the 2012 *Multimedia Computing and Systems (ICMCS), 2012 International Conference on*, 528-533.

Casey, E. (2009). *Handbook of digital forensics and investigation*: Academic Press.

Choi, J., Choi, K. and Lee, S. (2009). Evidence Investigation Methodologies for Detecting Financial Fraud Based on Forensic Accounting. Proceedings of the 2009 *Computer Science and its Applications, 2009. CSA'09. 2nd International Conference on*, 1-6.

Cicchetti, A., Ruscio, D., Kolovos, D. S. and Pierantonio, A. (2011). A test-driven approach for metamodel development. *Emerging Technologies for the Evolution and Maintenance of Software Models*, 319-342.

Cho, H. (2013). A demonstration-based approach for domain-specific modeling language creation. PhD dissertation, University of Alabama Libraries.

Cysneiros, L. M., Werneck, V., Amaral, J. and Yu, E. (2005). Agent/goal orientation versus object orientation for requirements engineering: A practical evaluation using an exemplar. Proceedings of the 2005 *Proc. of VIII Workshop in Requirements Engineering*, 123-134.

Daft, R. and Why, I. (1995). Why I recommended that your manuscript be rejected, and what you can do about it. *Publishing in the organizational sciences*, 1.

Djeddai, S., Strecker, M. and Mezghiche, M. (2012). Integrating a formal development for DSLs into meta-modeling. Proceedings of the 2012 *International Conference on Model and Data Engineering*, 55-66.

Eekels, J. and Roozenburg, N. F. (1991). A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. *Design Studies*, 12(4), 197-203.

Elhoseny, M., Hosny, A., Hassanien, A. E., Muhammad, K. and Sangaiah, A. K. (2017). Secure Automated Forensic Investigation for Sustainable Critical Infrastructures Compliant with Green Computing Requirements. *IEEE Transactions on Sustainable Computing*. 2377-3782.

Engelund, W. C., Stanley, D. O., Lepsch, R. A., McMillin, M. M. and Unal, R. (1993). Aerodynamic configuration design using response surface methodology analysis. *NASA STI/Recon Technical Report A*, 94.

Falkenberg, E., Hesse, W., Lindgreen, P., Nilsson, B., Oei, J., Rolland, C., et al. (1998). A Framework of Information Systems Concepts. The FRISCO Report, IFIP WG 8.1 Task Group FRISCO (Web edition).

Fasan, O. M. and Olivier, M. (2012a). Reconstruction in database forensics *Advances in Digital Forensics VIII* (pp. 273-287): Springer.

Fasan, O. M. and Olivier, M. S. (2012b). On Dimensions of Reconstruction in Database Forensics. Proceedings of the 2012c *WDFIA*, 97-106.

Fowler, K. (2008). *SQL server forenisc analysis*: Pearson Education.

Fowler, K., Gold, G. and MCSD, M. (2007). A real world scenario of a SQL Server 2005 database forensics investigation. *Information security reading room paper, SANS Institute*.

France, R. and Bieman, J. M. (2001). Multi-view software evolution: a UML-based framework for evolving object-oriented software. Proceedings of the 2001 *Software Maintenance, 2001. Proceedings. IEEE International Conference on*, 386-395.

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

Frühwirt, P., Kieseberg, P., Krombholz, K. and Weippl, E. (2014). Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations. *Digital Investigation*, 11(4), 336-348.

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

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

Gardner, T., Griffin, C., Koehler, J., and Hauser, R. (2003). *A review of OMG MOF 2.0 Query/Views/Transformations Submissions and Recommendations towards the final Standard.* Paper presented at the MetaModelling for MDA Workshop, 1-21.

Gargantini, A., Riccobene, E. and Scandurra, P. (2009). A semantic framework for metamodel-based languages. *Automated software engineering*, 16(3-4), 415-454.

Geisler, R., Klar, M. and Pons, C. (1998). *Dimensions and dichotomy in metamodeling*: Technische Universität Berlin, Fachbereich 13, Informatik.

Gillenson, M. L. (2008). *Fundamentals of database management systems*: John Wiley & Sons. p 366

Goerger, S. R. (2004). *Validating computational human behavior models: Consistency and accuracy issues.* Master Thesis, Monterey, California. Naval Postgraduate School.

Grobler, C., Louwrens, C. and von Solms, S. H. (2010). A framework to guide the implementation of proactive digital forensics in organisations. Proceedings of the 2010 *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, 677-682.

Guimaraes, M. A., Austin, R. and Said, H. (2010). Database forensics. Proceedings of the 2010 *2010 Information Security Curriculum Development Conference*, 62-65.

Guragain, K. K., Ledeczi, A. and Karsai, G. (2010). *Documentation Management and Generation for Domain-specific Models.* Master Thesis, Faculty of graduate School, Vanderbilt University.

Guizzardi, G. (2007). On ontology, ontologies, conceptualizations, modeling languages, and (meta) models. *Frontiers in artificial intelligence and applications*, 155, 18.

Haghighi, P. D., Burstein, F., Li, H. and Wang, C. (2013). Integrating Social Media with Ontologies for Real-Time Crowd Monitoring and Decision Support in Mass Gatherings. Proceedings of the 2013 *PACIS*, 64.

Hancock, M., Herbert, R. D. and Maher, C. G. (2009). A guide to interpretation of studies investigating subgroups of responders to physical therapy interventions. *Physical therapy*, 89(7), 698-704.

Hussein M. Hashi and Othman S.H, (2013), "Managing a Complexity of Physical Security Knowledge through a Physical Security Metamodel" in the International Symposium on Mathematical Sciences & Computing Research (iSMSC 2013), Ipoh, Perak, Malaysia

Hauger, W. K. and Olivier, M. S. (2015). The state of Database Forensic research. Proceedings of the 2015 *Information Security for South Africa (ISSA), 2015*, 1-8.

Hauksson, H. (2013). Metamodeling for Business Model Design : Facilitating development and communication of Business Model Canvas (BMC) models with an OMG standards-based metamodel, Master Thesis, School of Information and Communication Technology, KTH

Henderson-Sellers, B. (2011). Bridging metamodels and ontologies in software engineering. *Journal of Systems and Software*, 84(2), 301-313.

Hevner, A. R., March, S. T., Park, J. and Ram, S. (2004). Design science in information systems research. *MIS Q.*, 28(1), 75-105.

Adedayo, O. M. (2015). *Reconstruction in Database Forensics*. University of Pretoria.

Adedayo, O. M. and Olivier, M. S. (2015). Ideal log setting for database forensics reconstruction. *Digital Investigation*, 12, 27-40.

Ahmad, M. N., Colomb, R. M. and Sadiq, S. W. (2010). A UML profile for perdurant ontology of domain interlocking Institutional Worlds. *International Journal of Internet and Enterprise Management*, 6(3), 213-232.

Al-dhaqm, A., Razak, S., Othman, S. H., Ngadi, A., Ahmed, M. N. and Mohammed, A. A. (2017). Development and validation of a Database Forensic Metamodel (DBFM). *PloS one*, 12(2), e0170793.

Ali, A., Razak, S. A., Othman, S. H., Mohammed, A. and Saeed, F. (2017). A metamodel for mobile forensics investigation domain. *PloS one*, 12(4), e0176223.

Archer, L. (1984). Developments in design methodology: Chichester: Wiley.

Atkinson, C. and Kuhne, T. (2003). Model-driven development: a metamodeling foundation. *IEEE software*, 20(5), 36-41.

Azemovic, J. and Music, D. (2010). Methods for Efficient Digital Evidences Collecting of Business Proceses and Users Activity in eLearning Enviroments. Proceedings of the 2010 *e-Education, e-Business, e-Management, and e-Learning, 2010. IC4E'10. International Conference on*, 126-130.

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

Bandara, W., Indulska, M., Chong, S. and Sadiq, S. (2007). Major issues in business process management: an expert perspective.

Bassil, Y. (2012). A comparative study on the performance of the Top DBMS systems. *arXiv preprint arXiv:1205.2889*.

Basu, A. (2006). Forensic tamper detection in SQL server.

Becker, J., Rosemann, M. and Von Uthmann, C. (2000). Guidelines of business process modeling *Business Process Management* (pp. 30-49): Springer.

Beydoun, G., Low, G., Henderson-Sellers, B., Mouratidis, H., Gomez-Sanz, J. J., Pavó, J., et al. (2009a). FAML: a generic metamodel for MAS development. *Software Engineering, IEEE Transactions on*, 35(6), 841-863.

Beydoun, G., Low, G., Henderson-Sellers, B., Mouratidis, H., Gomez-Sanz, J. J., Pavon, J., et al. (2009b). FAML: a generic metamodel for MAS development. *IEEE Transactions on Software Engineering*, 35(6), 841-863.

Beyers, H., Olivier, M. and Hancke, G. (2011). Assembling metadata for database forensics *Advances in Digital Forensics VII* (pp. 89-99): Springer.

Beyers, H., Olivier, M. S. and Hancke, G. P. (2012). Arguments and Methods for Database Data Model Forensics. Proceedings of the 2012 *WDFIA*, 139-149.

Beyers, H. Q. (2013). DATABASE FORENSICS: INVESTIGATING COMPROMISED DATABASE MANAGEMENT SYSTEMS.

Beyers, H. Q. (2014). Database forensics: Investigating compromised database management systems.

Beyers, H. Q., Oliviery, M. S. and Hancke, G. P. (2014). Database application schema forensics. *South African Computer Journal*, 55, 1-11.

Bézivin, J. and Gerbé, O. (2001). Towards a precise definition of the OMG/MDA framework. Proceedings of the 2001 *Automated Software Engineering, 2001.(ASE 2001). Proceedings. 16th Annual International Conference on*, 273-280.

Bogen, A. C. (2006). *Selecting keyword search terms in computer forensics examinations using domain analysis and modeling*: Mississippi State University.

Buang, M. F. M. and Daud, S. M. (2012). A web-based KM system for digital forensics-knowledge sharing capability. Proceedings of the 2012 *Multimedia Computing and Systems (ICMCS), 2012 International Conference on*, 528-533.

Casey, E. (2009). *Handbook of digital forensics and investigation*: Academic Press.

Cho, H. (2013). *A demonstration-based approach for domain-specific modeling language creation.* University of Alabama Libraries.

Choi, J., Choi, K. and Lee, S. (2009). Evidence Investigation Methodologies for Detecting Financial Fraud Based on Forensic Accounting. Proceedings of the 2009 *Computer Science and its Applications, 2009. CSA'09. 2nd International Conference on*, 1-6.

Cysneiros, L. M., Werneck, V., Amaral, J. and Yu, E. (2005). Agent/goal orientation versus object orientation for requirements engineering: A practical evaluation using an exemplar. Proceedings of the 2005 *Proc. of VIII Workshop in Requirements Engineering*, 123-134.

Eekels, J. and Roozenburg, N. F. (1991). A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. *Design Studies*, 12(4), 197-203.

Fasan, O. M. and Olivier, M. (2012a). Reconstruction in database forensics *Advances in Digital Forensics VIII* (pp. 273-287): Springer.

Fasan, O. M. and Olivier, M. S. (2012b). On Dimensions of Reconstruction in Database Forensics. Proceedings of the 2012b *WDFIA*, 97-106.

Fowler, K. (2008). *SQL server forenisc analysis*: Pearson Education.

Fowler, K., Gold, G. and MCSD, M. (2007). A real world scenario of a SQL Server 2005 database forensics investigation. *Information security reading room paper, SANS Institute*.

Fruhwirt, P., Huber, M., Mulazzani, M. and Weippl, E. R. (2010). Innodb database forensics. Proceedings of the 2010 *Advanced Information Networking and*

Applications (AINA), 2010 24th IEEE International Conference on, 1028-1036.

Frühwirt, P., Kieseberg, P., Krombholz, K. and Weippl, E. (2014). Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations. *Digital Investigation*, 11(4), 336-348.

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

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

García-Holgado, A. and García-Peñalvo, F. J. (2017). A metamodel proposal for developing learning ecosystems. Proceedings of the 2017 *International Conference on Learning and Collaboration Technologies*, 100-109.

Goerger, S. R. (2004). *Validating computational human behavior models: Consistency and accuracy issues.* Monterey, California. Naval Postgraduate School.

Grobler, C., Louwrens, C. and von Solms, S. H. (2010). A framework to guide the implementation of proactive digital forensics in organisations. Proceedings of the 2010 *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, 677-682.

Guimaraes, M. A., Austin, R. and Said, H. (2010). Database forensics. Proceedings of the 2010 *2010 Information Security Curriculum Development Conference*, 62-65.

Guizzardi, G. (2007). On ontology, ontologies, conceptualizations, modeling languages, and (meta) models. *Frontiers in artificial intelligence and applications*, 155, 18.

Guragain, K. K., Ledeczi, A. and Karsai, G. (2010). *Documentation Management and Generation for Domain-specific Models.* Citeseer.

Hancock, M., Herbert, R. D. and Maher, C. G. (2009). A guide to interpretation of studies investigating subgroups of responders to physical therapy interventions. *Physical therapy*, 89(7), 698-704.

Hashi, H. A. and Othman, S. H. (2013). Managing a Complexity of Physical Security Knowledge through a Physical Security Metamodel.

Hauger, W. K. and Olivier, M. S. (2015). The state of Database Forensic research. Proceedings of the 2015 *Information Security for South Africa (ISSA), 2015*, 1-8.

Hauksson, H. and Johannesson, P. (2013). Metamodeling for Business Model Design. *Facilitating development and.*

Henderson-Sellers, B. (2011). Bridging metamodels and ontologies in software engineering. *Journal of Systems and Software*, 84(2), 301-313.

Jansen, W. A. and Delaitre, A. (2009). *Mobile forensic reference materials: A methodology and reification*: US Department of Commerce, National Institute of Standards and Technology.

Kelly, S. and Pohjonen, R. (2009). Worst practices for domain-specific modeling. *IEEE software*, 26(4).

Khanuja, H. and Suratkar, S. S. (2014). Role of metadata in forensic analysis of database attacks. Proceedings of the 2014 *Advance Computing Conference (IACC), 2014 IEEE International*, 457-462.

Khanuja, H. K. and Adane, D. (2012a). A framework for database forensic analysis. *Computer Science & Engineering: An International Journal (CSEIJ)*, 2(3), 27-41.

Khanuja, H. K. and Adane, D. (2013). Forensic Analysis of Databases by Combining Multiple Evidences. *International Journal Of Computers & Technology*, 7(3), 654-663.

Khanuja, H. K. and Adane, D. D. (2012b). A Framework For Database Forensic Analysis. *Published in Computer Science & Engineering: An International Journal (CSEIJ)*, 2(3).

Kleijnen, J. P. and Deflandre, D. (2006). Validation of regression metamodels in simulation: Bootstrap approach. *European journal of operational research*, 170(1), 120-131.

Kruse II, W. G. and Heiser, J. G. (2001). *Computer forensics: incident response essentials*: Pearson Education.

Kurtev, I. (2007). State of the art of QVT: A model transformation language standard. Proceedings of the 2007 *International Symposium on Applications of Graph Transformations with Industrial Relevance*, 377-393.

Lawrence, A. C. (2014). *Forensic Investigation of MySQL Database Management System.*

Lee, D., Choi, J. and Lee, S. (2009). Database forensic investigation based on table relationship analysis techniques. Proceedings of the 2009 *2009 2nd International Conference on Computer Science and Its Applications, CSA 2009*,

Lee, G. T., Lee, S., Tsomko, E. and Lee, S. (2007). Discovering Methodology and Scenario to Detect Covert Database System. Proceedings of the 2007 *Future Generation Communication and Networking (FGCN 2007)*, 130-135.

Lee, K. and Boddington, M. R. (2012). A Workflow to Support Forensic Database Analysis.

Lin, Y. (2004). *An efficient robust concept exploration method and sequential exploratory experimental design.* Georgia Institute of Technology.

Litchfield, D. (2007a). Oracle forensics part 1: Dissecting the redo logs. *NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd., Sutton.*

Litchfield, D. (2007b). Oracle forensics part 2: Locating dropped objects. *NGSSoftware Insight Security Research (NISR).*

Litchfield, D. (2007c). Oracle forensics part 4: Live response.

Litchfield, D. (2007d). 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. (2007e). 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. (2007f). Oracle forensics: Part 3 isolating evidence of attacks against the authentication mechanism. *NGSSoftware Insight Security Research (NISR).*

Litchfield, D. (2008). Oracle forensics part 7: using the Oracle system change number in forensic investigations. *Insight security research publication, NGSSoftware.*

Liu, C.-M. (2007). An electronic material flow control system for improving production efficiency in integrated-circuit packaging industry. Proceedings of the 2007 *RFID Eurasia, 2007 1st Annual*, 1-8.

Mokhtar, R., Rahman, A. A. and Othman, S. H. (2016). An Assessment-based Metamodel towards a Best Practice Assessment Model in Higher Education. *Indian Journal of Science and Technology*, 9(34).

Munk-Madsen, A. (2005). The Concept of a 'Project': A Proposal for a Unifying Definition. Proceedings of the 2005,

Nordstrom, G., Sztipanovits, J., Karsai, G. and Ledeczi, A. (1999). Metamodeling-rapid design and evolution of domain-specific modeling environments. Proceedings of the 1999 *Engineering of Computer-Based Systems, 1999. Proceedings. ECBS'99. IEEE Conference and Workshop on*, 68-74.

O'Leary, Z. (2004). *The essential guide to doing research*: Sage.

Oates, B. (2006). Researching Information Systems and Computing.: SAGE.

OGUTU, J. O. (2016). A Methodology to Test the Richness of Forensic Evidence of Database Storage Engine: Analysis of MySQL Update Operation in InnoDB and MyISAM Storage Engines

Olivier, M. S. (2009). On metadata context in database forensics. *Digital Investigation*, 5(3), 115-123.

Othman, S. H. (2013). Development of metamodel for information security risk management.

Othman, S. H. and Beydoun, G. (2010). A disaster management metamodel (DMM) validated. Proceedings of the 2010 *Pacific Rim Knowledge Acquisition Workshop*, 111-125.

Othman, S. H. and Beydoun, G. (2016). A metamodel-based knowledge sharing system for disaster management. *Expert Systems with Applications*, 63, 49-65.

Othman, S. H., Beydoun, G. and Sugumaran, V. (2014). Development and validation of a Disaster Management Metamodel (DMM). *Information Processing & Management*, 50(2), 235-271.

Palmer, G. (2001). A road map for digital forensic research. Proceedings of the 2001 *First Digital Forensic Research Workshop, Utica, New York*, 27-30.

Panesar-Walawege, R. K., Knutsen, T. S., Sabetzadeh, M. and Briand, L. C. (2011). CRESCO: Construction of Evidence Repositories for Managing Standards Compliance. Proceedings of the 2011 *ER Workshops*, 338-342.

Pavlou, K. (2011). Database forensics in the service of information accountability.

Pavlou, K. E. and Snodgrass, R. T. (2008). Forensic analysis of database tampering. *ACM Transactions on Database Systems (TODS)*, 33(4), 30.

Pavlou, K. E. and Snodgrass, R. T. (2010). The tiled bitmap forensic analysis algorithm. *Knowledge and Data Engineering, IEEE Transactions on*, 22(4), 590-601.

Pavlou, K. E. and Snodgrass, R. T. (2013). Generalizing database forensics. *ACM Transactions on Database Systems (TODS)*, 38(2), 12.

Peffers, K., Tuunanen, T., Rothenberger, M. A. and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77.

Pilone, D. and Pitman, N. (2005). *UML 2.0 in a Nutshell*: " O'Reilly Media, Inc.".

Poernomo, I. (2006). A type theoretic framework for formal metamodelling *Architecting Systems with Trustworthy Components* (pp. 262-298): Springer.

Quinn, B. and Arthur, C. (2011). PlayStation Network hackers access data of 77 million users. *The Guardian*, 27.

Rahayu, J. W., Chang, E., Dillon, T. S. and Taniar, D. (2000). A methodology for transforming inheritance relationships in an object-oriented conceptual model to relational tables. *Information and software Technology*, 42(8), 571-592.

Ramaswamy, C. and Sandhu, R. (1998). Role-based access control features in commercial database management systems. Proceedings of the 1998 *Proc. 21st Nat'l Information Systems Security Conf*, 503-511.

Rankins, R., Bertucci, P., Gallelli, C. and Silverstein, A. T. (2010). *Microsoft SQL server 2008 R2 unleashed*: Pearson Education.

Robson, C. (2002). *Real world research: A resource for social scientists and practitioner-researchers* (Vol. 2): Blackwell Oxford.

Sargent, R. G. (2005). Verification and validation of simulation models. Proceedings of the 2005 *Proceedings of the 37th conference on Winter simulation*, 130-143.

Sargent, R. G. (2015). Model Verification and Validation *Modeling and Simulation in the Systems Engineering Life Cycle* (pp. 57-65): Springer.

Schauerhuber, A., Wimmer, M. and Kapsammer, E. (2006). Bridging existing Web modeling languages to model-driven engineering: a metamodel for WebML. Proceedings of the 2006 *Workshop proceedings of the sixth international conference on Web engineering*, 5.

Selamat, S. R., Yusof, R. and Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, 8(10), 163-169.

Snodgrass, R. T., Yao, S. S. and Collberg, C. (2004). Tamper detection in audit logs. Proceedings of the 2004 *Proceedings of the Thirtieth international conference on Very large data bases-Volume 30*, 504-515.

Son, N., Lee, K.-g., Jeon, S., Chung, H., Lee, S. and Lee, C. (2011). The Method of Database Server Detection and Investigation in the Enterprise Environment *Secure and Trust Computing, Data Management and Applications* (pp. 164-171): Springer.

Susaimanickam, R. (2012). *A workflow to support forensic database analysis*. Murdoch University.

Takeda, H., Veerkamp, P. and Yoshikawa, H. (1990). Modeling design process. *AI magazine*, 11(4), 37.

Trabelsi, C., Atitallah, R. B., Meftali, S., Dekeyser, J.-L. and Jemai, A. (2011). A model-driven approach for hybrid power estimation in embedded systems design. *EURASIP Journal on Embedded Systems*, 2011(1), 569031.

Tripathi, S. and Meshram, B. B. (2012). Digital Evidence for Database Tamper Detection.

van Beers, W. C. (2005). Kriging metamodeling for simulation: Tilburg University, School of Economics and Management.

Von Alan, R. H., March, S. T., Park, J. and Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 28(1), 75-105.

Vrandečić, D. (2009). Ontology evaluation *Handbook on ontologies* (pp. 293-313): Springer.

Wachsmuth, G. (2007). Metamodel adaptation and model co-adaptation. Proceedings of the 2007 *European Conference on Object-Oriented Programming*, 600-624.

Wagner, J., Rasin, A. and Grier, J. (2015). Database forensic analysis through internal structure carving. *Digital Investigation*, 14, S106-S115.

Wagner, J., Rasin, A., Malik, T., Hart, K., Jehle, H. and Grier, J. (2017). Database Forensic Analysis with DBCarver. Proceedings of the 2017 *CIDR*,

Walls, J. G., Widmeyer, G. R. and El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. *Information systems research*, 3(1), 36-59.

Withers, R., Casson, R. and Shrimplin, A. (2002). Creating Web-based listings of electronic journals without creating extra work. *Library Collections, Acquisitions, and Technical Services*, 26(2), 107-112.

Wong, D. and Edwards, K. (2004). System and method for investigating a data operation performed on a database: Google Patents.

Wongthongtham, P., Chang, E. and Dillon, T. S. (2005). Towards' ontology'-based software engineering for multi-site software development. Proceedings of the 2005 *Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on*, 362-365.

Wright. (2007). Oracle forensics in a nutshell. 2007.

Wright, P. M. (2005). Oracle database forensics using LogMiner. Proceedings of the 2005 *June 2004 Conference, SANS Institute*,

Yoon, J., Jeong, D., Kang, C.-h. and Lee, S. (2016). Forensic investigation framework for the document store NoSQL DBMS: MongoDB as a case study. *Digital Investigation*, 17, 53-65.

Yusoff, Y., Ismail, R. and Hassan, Z. (2011a). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology (IJCSIT)*, 3(3), 17-31.

Yusoff, Y., Ismail, R. and Hassan, Z. (2011b). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology*, 3(3), 17-31.

Ivanov, P. and Voigt, K. (2011). Schema, ontology and metamodel matching-different, but indeed the same? Proceedings of the 2011 *International Conference on Model and Data Engineering*, 18-30.

Jansen, W. A. and Delaitre, A. (2009). *Mobile forensic reference materials: A methodology and reification*: US Department of Commerce, National Institute of Standards and Technology, 1-31.

Karie, N. M. and Venter, H. S. (2013). Resolving Terminology Heterogeneity in Digital Forensics Using the Web. Proceedings of the 2013 *Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013*, 328.

Kelly, S. and Pohjonen, R. (2009). Worst practices for domain-specific modeling. *IEEE software*, 26(4), 22-29.

Kent, S. (2002). Model driven engineering. Proceedings of the 2002 *Integrated formal methods*, 286-298.

Khanuja, H. and Suratkar, S. S. (2014). Role of metadata in forensic analysis of database attacks. Proceedings of the 2014 *Advance Computing Conference (IACC), 2014 IEEE International*, 457-462.

Khanuja, H. K. and Adane, D. (2013). Forensic Analysis of Databases by Combining Multiple Evidences. *International Journal Of Computers & Technology*, 7(3), 654-663.

Khanuja, H. K. and Adane, D. D. (2012). A Framework For Database Forensic Analysis. *Published in Computer Science & Engineering: An International Journal (CSEIJ)*, 2(3).

Kleijnen, J. P. and Deflandre, D. (2006). Validation of regression metamodels in simulation: Bootstrap approach. *European journal of operational research*, 170(1), 120-131.

Koch, N. and Kraus, A. (2003). Towards a common metamodel for the development of web applications. *Lecture notes in computer science*, 497-506.

Kruse II, W. G. and Heiser, J. G. (2001). *Computer forensics: incident response essentials*: Pearson Education.

Kuechler, B. and Vaishnavi, V. (2008). On theory development in design science research: anatomy of a research project. *European Journal of Information Systems*, 17(5), 489-504.

Kurtev, I. (2007). State of the art of QVT: A model transformation language standard. Proceedings of the 2007 *International Symposium on Applications of Graph Transformations with Industrial Relevance*, 377-393.

Lalla, H. and Flowerday, S. (2010). Towards a Standardised Digital Forensic Process: E-mail Forensics. Jounral of Forensic Sciences, 59(5), 1231-1241

Lawrence, A. C. (2014). Forensic Investigation of MySQL Database Management System. Bachelor Thesis, Computer Science and Computer Engineering, University of Arkansas

Lee, D., Choi, J. and Lee, S. (2009). Database forensic investigation based on table relationship analysis techniques. Proceedings of the *2nd International Conference on Computer Science and Its Applications, CSA.*

Lee, G. T., Lee, S., Tsomko, E. and Lee, S. (2007). Discovering Methodology and Scenario to Detect Covert Database System. Proceedings of the *Future Generation Communication and Networking (FGCN 2007)*, 130-135.

Levendovszky, T., Rumpe, B., Schätz, B. and Sprinkle, J. (2010). Model Evolution and Management *Model-Based Engineering of Embedded Real-Time Systems* (pp. 241-270): Springer.

Lin, Y. (2004). *An efficient robust concept exploration method and sequential exploratory experimental design.* PhD Thesis, Georgia Institute of Technology.

Litchfield, D. (2007a). Oracle forensics part 1: Dissecting the redo logs. *NGSSoftware Insight Security Research (NISR), 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.*

Litchfield, D. (2007d). Oracle forensics part 4: Live response. *NGSSoftware Insight Security Research (NISR) Publication, Next Generation Security Software.*

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. (2007g). Oracle forensics: Part 3 isolating evidence of attacks against the authentication mechanism. *NGSSoftware Insight Security Research (NISR).*

Litchfield, D. (2008). Oracle forensics part 7: using the Oracle system change number in forensic investigations. *Insight security research publication, NGSSoftware.*

Liu, C.-M. (2007). An electronic material flow control system for improving production efficiency in integrated-circuit packaging industry. Proceedings of the 2007 *RFID Eurasia, 2007 1st Annual*, 1-8.

Lu, S. and Tcheng, D. (1991). Building layered models to support engineering decision making: A machine learning approach. *Urbana*, 51, 61801.

Lutui, R. (2016). A multidisciplinary digital forensic investigation process model. *Business Horizons*, 59(6), 593-604.

Mens, T. and Van Gorp, P. (2006). A taxonomy of model transformation. *Electronic Notes in Theoretical Computer Science*, 152, 125-142.

Mokhtar, R., Rahman, A. A. and Othman, S. H. (2016). An Assessment-based Metamodel towards a Best Practice Assessment Model in Higher Education. *Indian Journal of Science and Technology*, 9(34), 1-11.

Montasari, R. (2016). A comprehensive digital forensic investigation process model. *International Journal of Electronic Security and Digital Forensics*, 8(4), 285-302.

Muliawan, O., Van Gorp, P., Keller, A. and Janssens, D. (2008). Executing a standard compliant transformation model on a non-standard platform. Proceedings of the 2008 *Software Testing Verification and Validation Workshop, 2008. ICSTW'08. IEEE International Conference on*, 151-160.

Ralph P., Wand Y. (2009) A Proposal for a Formal Definition of the Design Concept. In: Lyytinen K., Loucopoulos P., Mylopoulos J., Robinson B. (eds) Design Requirements Engineering: A Ten-Year Perspective. Lecture Notes in Business Information Processing, vol 14. Springer, Berlin, Heidelberg

Myers, J. (2005). Data security in a semantic data model: Google Patents.

Nordstrom, G., Sztipanovits, J., Karsai, G. and Ledeczi, A. (1999). Metamodeling-rapid design and evolution of domain-specific modeling environments. Proceedings of the 1999 *Engineering of Computer-Based Systems, 1999. Proceedings. ECBS'99. IEEE Conference and Workshop on*, 68-74.

O'Leary, Z. (2004). *The essential guide to doing research*: Sage.

Oates, B. (2006). Researching Information Systems and Computing.: Sage.

Ogutu, J. O. (2016). A Methodology to Test the Richness of Forensic Evidence of Database Storage Engine: Analysis of MySQL Update Operation in InnoDB and MyISAM Storage Engines, 90-105.

Olivier, M. S. (2009). On metadata context in database forensics. *Digital Investigation*, 5(3), 115-123.

Oppel, A. (2009). *Databases A Beginner's Guide*: McGraw-Hill, Inc.

Othman, S. H. (2012). Metamodeling Approach for Managing Disaster Management Knowledge.

Othman, S. H. (2013). Development of metamodel for information security risk management.

Othman, S. H. and Beydoun, G. (2010). A disaster management metamodel (DMM) validated. Proceedings of the 2010 *Pacific Rim Knowledge Acquisition Workshop*, 111-125.

Othman, S. H. and Beydoun, G. (2013). Model-driven disaster management. *Information & Management*, 50(5), 218-228.

Othman, S. H. and Beydoun, G. (2016). A metamodel-based knowledge sharing system for disaster management. *Expert Systems with Applications*, 63, 49-65.

Othman, S. H., Beydoun, G. and Sugumaran, V. (2014). Development and validation of a Disaster Management Metamodel (DMM). *Information Processing & Management*, 50(2), 235-271.

Paige, R. F., Brooke, P. J. and Ostroff, J. S. (2004). Specification-driven development of an executable metamodel in Eiffel. *WISME'04*.

Pakhira, M. K. (2012). *Database Management System*: PHI Learning Pvt. Ltd.

Palmer, G. (2001). A road map for digital forensic research. Proceedings of the 2001 *First Digital Forensic Research Workshop, Utica, New York*, 27-30.

Panesar-Walawege, R. K., Knutsen, T. S., Sabetzadeh, M. and Briand, L. C. (2011). CRESCO: Construction of Evidence Repositories for Managing Standards Compliance. Proceedings of the 2011 *ER Workshops*, 338-342.

Pavlou, K. E. (2012). *Database forensics in the service of information accountability*: The University of Arizona, 30-35.

Pavlou, K. E. and Snodgrass, R. T. (2008). Forensic analysis of database tampering. *ACM Transactions on Database Systems (TODS)*, 33(4), 30.

Pavlou, K. E. and Snodgrass, R. T. (2010). The tiled bitmap forensic analysis algorithm. *Knowledge and Data Engineering, IEEE Transactions on*, 22(4), 590-601.

Pavlou, K. E. and Snodgrass, R. T. (2013). Generalizing database forensics. *ACM Transactions on Database Systems (TODS)*, 38(2), 12.

Peffers, K., Tuunanen, T., Rothenberger, M. A. and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77.

Pilone, D. and Pitman, N. (2005). *UML 2.0 in a Nutshell*: " O'Reilly Media, Inc.".

Poernomo, I. (2006). A type theoretic framework for formal metamodeling *Architecting Systems with Trustworthy Components* (pp. 262-298): Springer.

Quinn, B. and Arthur, C. (2011). PlayStation Network hackers access data of 77 million users. *The Guardian*, 27.

Rahayu, J. W., Chang, E., Dillon, T. S. and Taniar, D. (2000). A methodology for transforming inheritance relationships in an object-oriented conceptual model to relational tables. *Information and software Technology*, 42(8), 571-592.

Rankins, R., Bertucci, P., Gallelli, C. and Silverstein, A. T. (2010). *Microsoft SQL server 2008 R2 unleashed*: Pearson Education.

Robson, C. (2002). *Real world research: A resource for social scientists and practitioner-researchers* (Vol. 2): Blackwell Oxford.

Rose, L. M., Kolovos, D. S., Paige, R. F. and Polack, F. A. (2010). Model migration with epsilon flock. Proceedings of the 2010 *International Conference on Theory and Practice of Model Transformations*, 184-198.

Sadilek, D. A. and Weißleder, S. (2008). Towards Automated Testing of Abstract Syntax Specifications of Domain-Specific Modeling Languages. Proceedings of the 2008 *DSML*, 21-29.

Sargent, R. G. (2005). Verification and validation of simulation models. Proceedings of the 2005 *Proceedings of the 37th conference on Winter simulation*, 130-143.

Sargent, R. G. (2015). Model Verification and Validation *Modeling and Simulation in the Systems Engineering Life Cycle* (pp. 57-65): Springer.

Selamat, S. R., Yusof, R. and Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, 8(10), 163-169.

Shan, W. and Shixuan, S. (2008). Introduction to database system: Higher Education Press. Beijing, China.

Shirvani, F. (2016). Selection and Application of MBSE Methodology and Tools to Understand and Bring Greater Transparency to the Contracting of Large Infrastructure Projects. School of Computing and Information Technology, University of Wollongong

Singh, S. K. (2011). *Database systems: Concepts, design and applications*: Pearson Education India.

Smolik, P. C. (2006). Mambo Metamodeling Environment. *Library of the Faculty of Information Technology, Brno University of Technology, Czech Republic*.

Snodgrass, R. T., Yao, S. S. and Collberg, C. (2004). Tamper detection in audit logs. Proceedings of the 2004 *Proceedings of the Thirtieth international conference on Very large data bases-Volume 30*, 504-515.

Son, N., Lee, K.-g., Jeon, S., Chung, H., Lee, S. and Lee, C. (2011). The Method of Database Server Detection and Investigation in the Enterprise Environment *Secure and Trust Computing, Data Management and Applications* (pp. 164-171): Springer.

Štuikys, V. and Damaševičius, R. (2013). A model-driven view to meta-program development process *Meta-Programming and Model-Driven Meta-Program Development* (pp. 127-142): Springer.

Susaimanickam, R. (2012). *A workflow to support forensic database analysis.* Master Dessertation, Murdoch University. Faculty of Law, Business and Information Technology.

Takeda, H., Veerkamp, P. and Yoshikawa, H. (1990). Modeling design process. *AI magazine*, 11(4), 37.

Trabelsi, C., Atitallah, R. B., Meftali, S., Dekeyser, J.-L. and Jemai, A. (2011). A model-driven approach for hybrid power estimation in embedded systems design. *EURASIP Journal on Embedded Systems*, 2011(1), 569031.

Tripathi, S. and Meshram, B. B. (2012). Digital Evidence for Database Tamper Detection. *Journal of Information Security*, 3, 113.

van Beers, W. C. (2005). Kriging metamodeling for simulation: Tilburg University, School of Economics and Management, Tilburg University Press

Von Alan, R. H., March, S. T., Park, J. and Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 28(1), 75-105.

Vrandečić, D. (2009). Ontology evaluation *Handbook on ontologies* (pp. 293-313): Springer.

Wachsmuth, G. (2007). Metamodel adaptation and model co-adaptation. Proceedings of the 2007 *European Conference on Object-Oriented Programming*, 600-624.

Wagner, J., Rasin, A. and Grier, J. (2015). Database forensic analysis through internal structure carving. *Digital Investigation*, 14, S106-S115.

Wagner, J., Rasin, A., Malik, T., Heart, K., Jehle, H., and Grier, J. (2017). *Database forensic analysis with DBCarver.* Paper presented at the CIDR 2017, 8th Biennial Conference on Innovative Data Systems Research, 1-10.

Walls, J. G., Widmeyer, G. R. and El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. *Information systems research*, 3(1), 36-59.

Watson, R. T. (2008). *Data management, databases and organizations*: John Wiley & Sons.

Whittle, J. (2002). Workshops and Tutorials at the UML 2002 Conference. Proceedings of the 2002 *International Conference on the Unified Modeling Language*, 442-447.

Withers, R., Casson, R. and Shrimplin, A. (2002). Creating Web-based listings of electronic journals without creating extra work. *Library Collections, Acquisitions, and Technical Services*, 26(2), 107-112.

Wong, D. and Edwards, K. (2004). System and method for investigating a data operation performed on a database: Google Patents.

Wongthongtham, P., Chang, E. and Dillon, T. S. (2005). Towards' ontology'-based software engineering for multi-site software development. Proceedings of the 2005 *Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on*, 362-365.

Wright. (2007). Oracle forensics in a nutshell. 2007. http://www.databasesecurity.com/dbsec/OracleForensicsInANutshell.pdf.

Wright, P. and Burleson, D. (2008). Oracle Forensics: Oracle Security Best Practices (Oracle In-Focus series): Paperback, 1-200.

Wright, P. M. (2005). Oracle database forensics using LogMiner. Proceedings of the 2005 *June 2004 Conference, SANS Institute*,

Yoon, J., Jeong, D., Kang, C.-h. and Lee, S. (2016). Forensic investigation framework for the document store NoSQL DBMS: MongoDB as a case study. *Digital Investigation*, 17, 53-65.

Yusoff, Y., Ismail, R. and Hassan, Z. (2011). Common phases of computer forensics investigation models. International Journal of Computer Science & Information Technology (IJCSIT), 3(3), 17-31.

LIST OF PUBLICATIONS

Journal with Impact Factors

1. Al-Dhaqm, A., Razak, S., Othman, S. H., Ngadi, A., Ahmed, M. N., & Mohammed, A. A. (2017). Development and validation of a Database Forensic Metamodel (DBFM). PloS one, 12(2), e0170793. Q1 IF = 2.86

2. Al-Dhaqm, Arafat, Shukor Razak, Siti Hajar Othman, Kim-Kwang Raymond Choo, William Bradley Glisson, Abdulalem Ali, and Mohammad Abrar. "CDBFIP: Common Database Forensic Investigation Processes for Internet of Things." IEEE Access 5 (2017): 24401-24416. Q1, IF = 3.557.

3. Al-Dhaqm, Arafat, Shukor Abd Razak, Siti Hajar Othman, Asri Nagdi, and Abdulalem Ali. "A generic database forensic investigation process model." Jurnal Teknologi 78, no. 6-11 (2016): 45-57. Scopus Index

Indexed Journal (SCOPUS)

1. Al-Dhaqm, Arafat, Shukor Abd Razak, Siti Hajar Othman, Asri Nagdi, and Abdulalem Ali. "A generic database forensic investigation process model." Jurnal Teknologi 78, no. 6-11 (2016): 45-57.

2. Aldhaqm, Aarafat, Shukor Abd Razak, Siti Hajar Othman, Abdulalem Ali, and Asri Ngadi. "Research Article Conceptual Investigation Process Model for Managing Database Forensic Investigation Knowledge." (2016).

Indexed Conference Proceeding

1. Aldhaqm, Aarafat, Shukor Abd Razak, Siti Hajar Othman. "Common Investigation Process Model for Database Forensic Investigation Discipline". 1 st ICRIL-International Conference on Innovation in Science and Technology (IICIST 2015).

2. Al-Dhaqm, Arafat, Shukor Abd Razak, Siti Hajar Othman, Asri Ngadi. (2018). Model Derivation System to Manipulate Database Forensic Investigation Domain Knowledge.