infrastructures

MDPI

Article

Face Validation of Database Forensic Investigation Metamodel

Arafat Al-Dhaqm [1,2], Shukor Razak [1], Richard A. Ikuesan [3], Victor R. Kebande [4,5,*] and Siti Hajar Othman [1]

[1] Faculty of Engineering, School of Computing, Computer Science Department, Universiti Teknologi Malaysia (UTM), Skudai 81310, Johor, Malaysia; mrarafat@utm.my (A.A.-D.); shukorar@utm.my (S.R.); hajar@utm.my (S.H.O.)
[2] Computer Science Department, Aden Community College, Aden 999101, Yemen
[3] Department of Cybersecurity and Networking, School of Information Technology, Community College Qatar, Doha 7344, Qatar; richard.ikuesan@ccq.edu.qa
[4] Department of Computer Science and Media Technology Department, Malmö Universitet, Nordenskiöldsgatan 1, 21119 Malmö, Sweden
[5] Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 97187 Luleå, Sweden
* Correspondence: victor.kebande@mau.se or victor.kebande@ltu.se

Abstract: Using a face validity approach, this paper provides a validation of the Database Forensic Investigation Metamodel (DBFIM). The DBFIM was developed to solve interoperability, heterogeneity, complexity, and ambiguity in the database forensic investigation (DBFI) field, where several models were identified, collected, and reviewed to develop DBFIM. However, the developed DBFIM lacked the face validity-based approach that could ensure DBFIM's applicability in the DBFI field. The completeness, usefulness, and logic of the developed DBFIM needed to be validated by experts. Therefore, the objective of this paper is to perform the validation of the developed DBFIM using the qualitative face validity approach. The face validity method is a common way of validating metamodels through subject expert inquiry on the domain application of the metamodel to assess whether the metamodel is reasonable and compatible based on the outcomes. For this purpose, six experts were nominated and selected to validate the developed DBFIM. From the expert review, the developed DBFIM was found to be complete, coherent, logical, scalable, interoperable, and useful for the DBFI field.

Keywords: database forensics; digital forensic; face validity; metamodel; validation

check for updates

Citation: Al-Dhaqm, A.; Razak, S.; Ikuesan, R.A.; R. Kebande, V.; Hajar Othman, S. Face Validation of Database Forensic Investigation Metamodel. *Infrastructures* **2021**, *6*, 13. https://doi.org/10.3390/infrastructures6020013

Received: 20 December 2020
Accepted: 14 January 2021
Published: 20 January 2021

1. Introduction

Database forensic investigation (DBFI) is an important field for identifying and detecting database-related crimes. Moreover, this field is heterogeneous and interoperable, owing to its variety and the multidimensional nature of the database systems [1]. Database systems can be classified into three dimensions; compromised databases, destroyed databases, and changed databases [2]. The Compromised Database Dimension refers to a database incident where some metadata or database management system (DBMS) software have been modified by an attacker even though the database is still operational [2]. Next, the Destroyed Database Dimension refers to databases where data or data files may have been modified, deleted, or copied from their original location. These databases may or may not be operational depending on the extent of the damage [2]. Lastly, the Modified Database Dimension covers databases that have not been compromised or damaged but have undergone changes due to normal business processes since the event of interest occurred [2].

Due to the diversity and multidimensional nature of database systems, [3] in 2017 developed a comprehensive/generic framework called the Database Forensic Investigation Metamodel (DBFIM) to solve heterogeneity, interoperability, complexity, and ambiguity in the DBFI field. The developed DBFIM identified, recognized, extracted, and matched different DBFI processes, concepts, activities, and tasks from different DBFI models into a developed metamodel that allowed practitioners to easily derive solution models.

However, the developed metamodel was not validated by subject matter experts to demonstrate its applicability and effectiveness in the DBFI field. Hence, this paper aims to validate the developed DBFIM using the qualitative face validity method. The face validity method asks individuals knowledgeable about the domain application whether the metamodel is reasonable and compatible [4]. The common method of validating metamodels is through face validation using a subject matter expert [5]. This validation technique is more effective than other validation techniques. For this purpose, six experts were nominated and selected to validate the developed DBFIM from the modeling and digital forensic investigation perspectives to ensure its completeness, clearness, logicalness, scalability, interoperability, and usefulness. Structured interviews were adapted with common questions for each interviewee.

The remainder of this paper is organized into six sections as follows: Section 2 presents the study background and related works in the DBFI field. Section 3 presents the developed DBFIM, while Section 4 discusses the methodology. Results of validations are presented in Section 5. Discussion on the developed DBFIM is offered in Section 6. The conclusion and ideas for future works are presented in Section 6.

2. Background and Related Works

The DBFI field is not similar to other digital forensic fields such as mobile forensics, network forensics, or computer forensics. The DBFI field deals with database systems from three dimensions, where the other digital forensic fields deal with one dimension, the system file dimension [6]. Thus, the DBFI field lacks a multidimensional nature and a variety of database systems. This produces many issues and challenges in the DBFI field, such as redundant forensic models, processes, concepts, operations, tasks, and policies. In addition, there is a lack of universal forensic investigation tools and unified investigation frameworks.

Several works have been proposed in the DBFI literature by various researchers. For example, an investigation process model was developed by [7] that used processes and activities to discover information about an operation performed on a database [6]. Additionally, the Log Miner tool was developed by [8] to reconstruct actions taken on an Oracle database even when auditing features have been turned off. In addition, Litchfield offered a series of technical models [9–15] to deal with several specific Oracle database incidents, cases, and scenarios. Additionally, a database forensic analysis model was proposed by [16] to reconstruct database activities through internal structure carving via the reconstruction of volatile artifacts and the recovery of database schema. However, this model could only reconstruct volatile artifacts. A forensic methodology for testing the tracks of any storage engine on the internal files of a DBMS was proposed by [17], which helps in flagging and listing files that have been affected by a particular database operation. These files can then be analyzed to interpret their actual content to see the nature of the change and determine the worth of the evidence. This model provides three investigation stages—preliminary analysis, execution, and analysis—but can only be used on MySQL database systems. [18] proposed a reconstruction model for rebuilding database content from a database image without using any log or system metadata. A special forensic tool called "DBCarver" was proposed for this task that permits the reconstruction of database storage. Therefore, all existing DBFI models are specific and have redundant processes. [19] proposed a common investigation process model for the DBFI field that consisted of four main processes: (1) identification; (2) artifact collection; (3) artifact analysis; and (4) documentation and presentation. [20] proposed a model derivation system to instantiate solution models from the metamodel (DBFIM) developed by [3] in 2017. In addition, [21] explored the techniques that can be utilized to perform forensic investigations of compromised MySQL databases. The use of simulated investigative scenarios to assist forensic investigative processes has produced positive results.

Recently, several works have been proposed in the literature for the DBFI field. For example, [21] introduced methods that can be applied to perform forensic investigations of a compromised MySQL database. The proposed method was introduced based on three simulation scenarios. These were then tracked in order to arrive at each of the testing processes that were performed, then, eventually a significant assessment of the propositions was given. Consequently, [22] proposed a forensic methodology to obtain and normalize various audit logs in a consistent XML format, which are obtained from different databases. The main goal of the proposed methodology is to examine database operations and to deliver information responsibility to databases [23]. A broad literature review that assists field researchers in comprehending the DBFI domain was provided and all existing DBFI works were analyzed and discussed, and some solutions were suggested for the limitations that were identified. Apart from that, [24] proposed a unified incident response framework which can be relied upon in the DBFI domain. It comprises three main phases: the pre-incident response, during-incident response, and post-incident response. It is a hybrid framework that comprises four main objectives: create a strategy to prevent any database failure, examine and explore for possible evidence, retrieve database actions, and finally distribute database disaster information. A survey work on the database forensic investigation processes was provided by [25]. They highlighted three common limitations of the DBFI domain, as follows: (1) redundant and irrelevant investigation processes; (2) redundant and irrelevant investigation concepts and terminologies; and (3) a lack of unified models to manage, share, and reuse DBFI knowledge. Moreover, they suggested three solutions for the discovered limitations, as follows: (1) propose generic DBFI process/model for the DBFI field; (2) develop a semantic metamodeling language to structure, manage, organize, share, and reuse DBFI knowledge; and (3) develop a repository to store and retrieve DBFI field knowledge. Nevertheless, a forensic model proposed by [26] for mobile database encryption forensics investigation in Android smartphones based on static analysis, which is not limited to a specific mobile application, features automated analytics. The model uses the installation package of the Android application to perform reverse analysis, constructs an inter-program control flow chart, and builds a data flow graph based on the control flow graph. [27] proposed a security and privacy preservation framework for cloud computing-based face detection and resolution framework in IoT. The identity authentication scheme, data encryption scheme, and data integrity checking scheme are proposed to meet the demands of confidentiality, integrity, and availability in the processes of face identification and face resolution, which could play a key role in the databases.

3. Database Forensic Investigation Metamodel

The DBFIM was developed using a metamodeling approach in order to solve interoperability, heterogeneity, complexity, and ambiguity in the DBFI field [3]. The developed DBFIM was previously validated from the generality and expressiveness perspectives through comparisons with other models [28], and frequency-based selection [29]. From the generality perspective DBFIM was validated to ensure the coverage of existing DBFI field models and direct coverage of real-world concepts, however, face validation for the DBFIM was not conducted for purposes of ensuring its applicability, completeness, coherence, logicalness, scalability, interpretability, and usefulness, where Figures 1–4 shows the developed DBFIM.

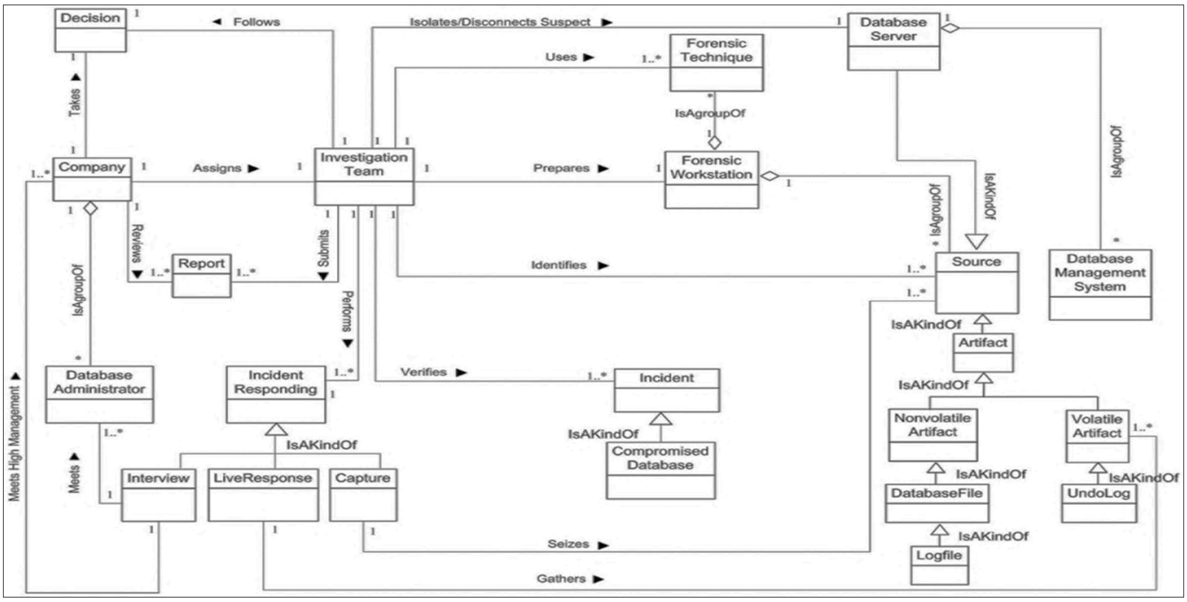

Figure 1. Database Forensic Investigation Metamodel (DBFIM) identification (Class 1).

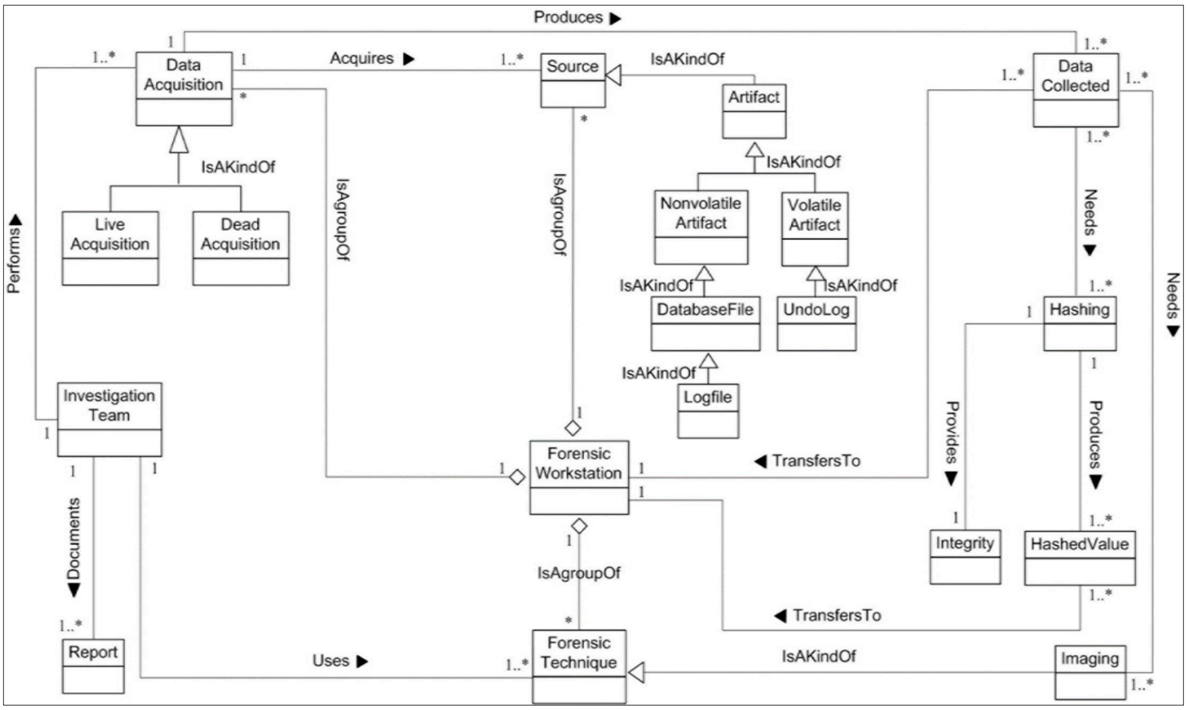

Figure 2. DBFIM artifact collection (Class 2).

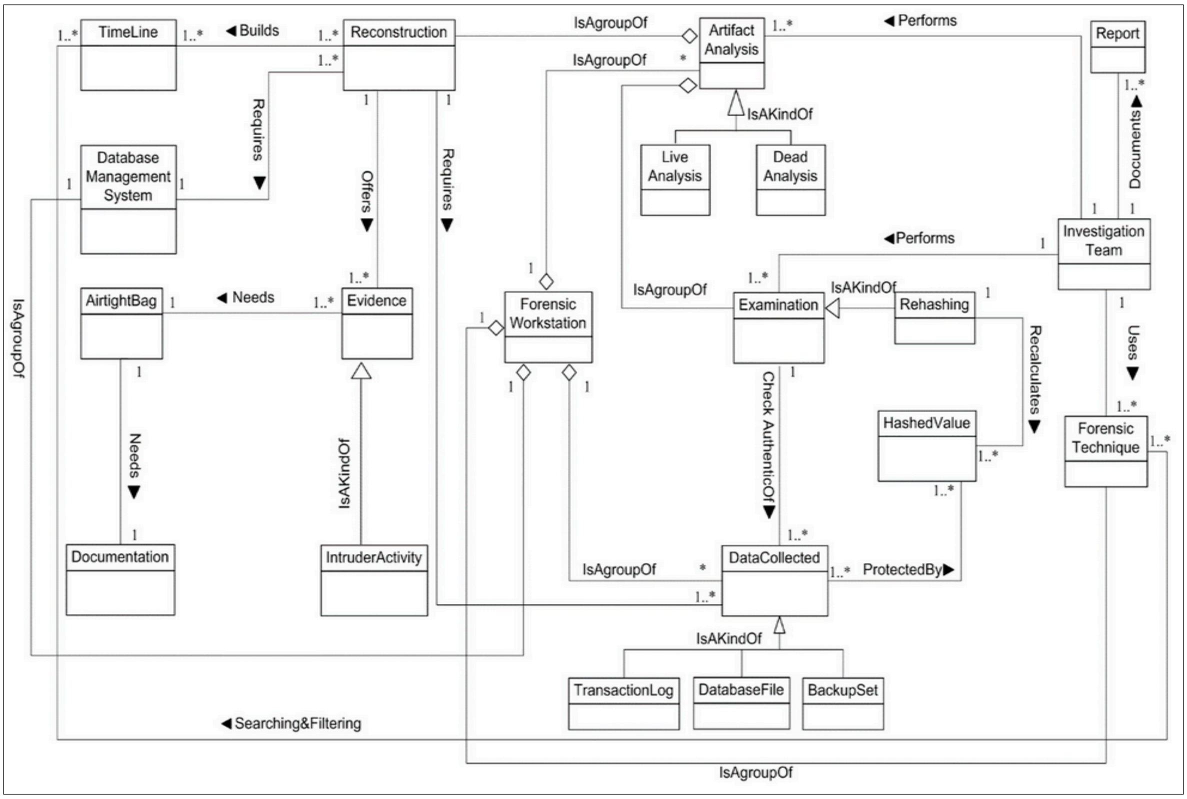

Figure 3. DBFIM artifact analysis (Class 3).

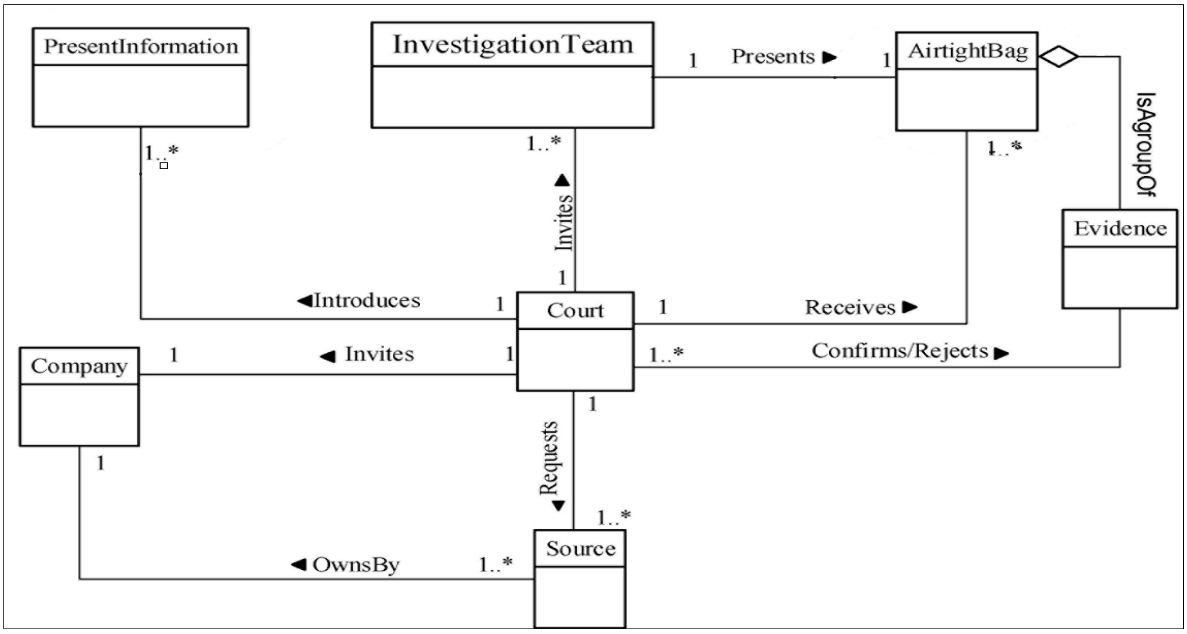

Figure 4. DBFIM documentation and presentation (Class 4).

4. Methodology

To validate the proposed DBFIM, which was previously highlighted in Section 3, a suitable method adapted from [28] was applied, which consists of two main phases, as shown in Figure 5: Given that the face validity approach is more of an exploratory research, the qualitative research approach is preferred, given that it allows the DBFIM expert validators to air their thoughts, perceptions, clarity, and actions with regard to the metamodel. This allows one to have an understanding on how the model could be improved.

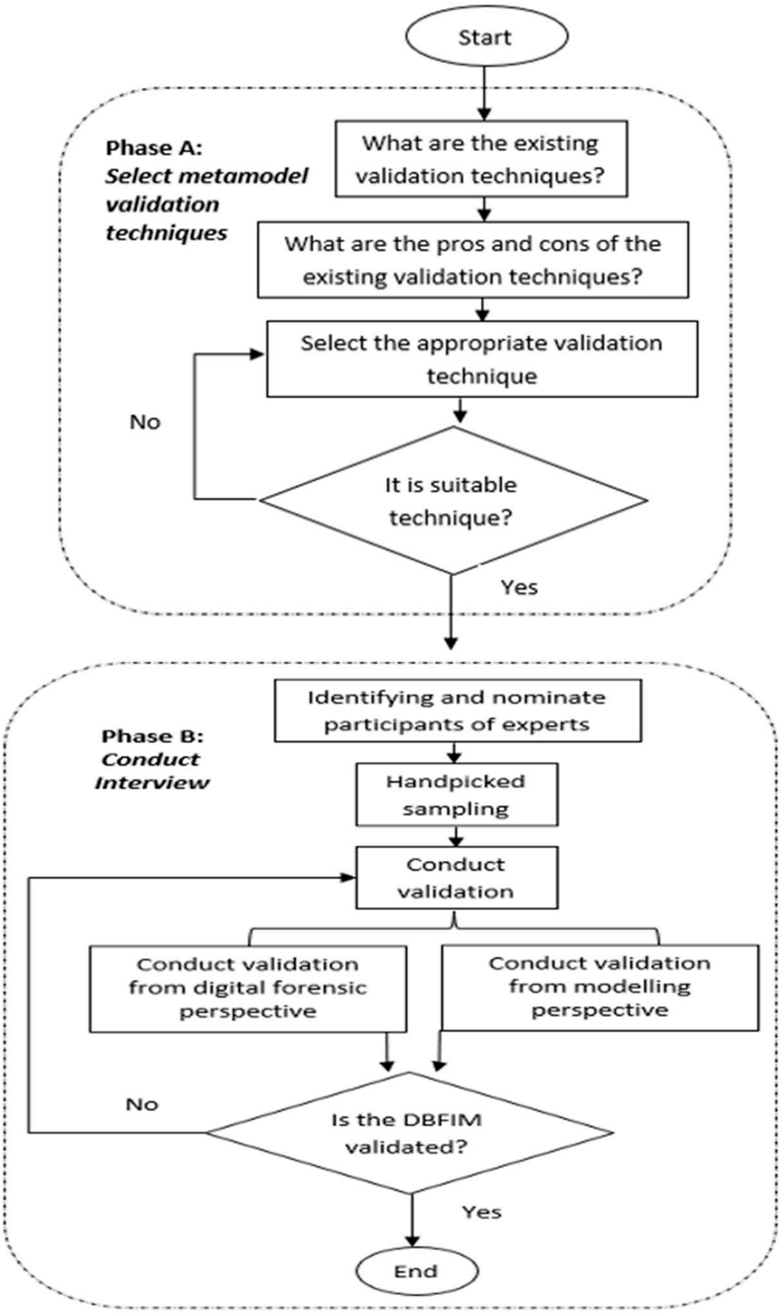
Start
Phase A:
Select metamodel validation techniques
What are the existing validation techniques?
What are the pros and cons of the existing validation techniques?
Select the appropriate validation technique
No
It is suitable technique?
Yes
Phase B:
Conduct Interview
Identifying and nominate participants of experts
Handpicked sampling
Conduct validation
Conduct validation from digital forensic perspective
Conduct validation from modelling perspective
No
Is the DBFIM validated?
Yes
End

Figure 5. Metamodel validation [28].

4.1. Phase A (Figure 5a)*: Select Metamodel Validation Techniques: This Phase Aims to Find the Proper Validation Techniqe to Validate the Proposed DBFIM. To Find the Proper/Appropriate Validation Technique, This Study Should Answer These Two Quesisions*

1. What are the existing metamodel validation techniques?
2. What are the pros and cons of the existing metamodel validation techniques?

As this step aims to select the proper metamodel validation technique to verify the completeness, logicalness, coherence, scalability, and usefulness of the developed DBFIM, a list of existing metamodel validation techniques and the advantages and disadvantages of these techniques are highlighted in this phase. Metamodels need to be validated before being utilized as a representation of real application domains. The quality of a metamodel is measured in view of how the metamodel can satisfy requirements during its creation [30]. In order to satisfy the completeness and effectiveness of the developed DBFIM, several validation techniques were applied during the validation stage. When the metamodel was developed, the question of how the metamodel can be used for real word problems is often asked. According to [31], the criteria to select the best type of validation technique can be determined according to metamodel type and the goal of its development (e.g., agent-based modeling, semantic and conceptual modeling, and mathematical and statistical modeling). Table 1 shows several of the validation techniques used to validate the metamodel. For example, the bootstrap approach [32], cross-validation [33] and multistage validation [4] are usually used for the validation of simulation metamodels. These approaches involve a few cycles of comparison and need a large sample size to achieve validity. Since the DBFI models used in the developed DBFIM are limited and the size of the sample is small, these validation approaches were not suitable. With a smaller sample size, comparison against other models [4], which does not require a large sample to achieve validity, was more suitable. This study also needed to evaluate the completeness, logicalness, coherence, scalability, and usefulness of the metamodel. Thus, the face validity technique [4] was used and full domain experts were consulted to confirm that the metamodel represented the domain correctly. The process of validating the metamodel is not yet well defined due to the following reasons [5]: the lack of a robust set of environmental data to run behavioral models for model validation and no uniform method of validating cognitive models. Therefore, this paper validates the developed DBFIM, similarly to [34–37], by using face validity.

Face validity asks individuals knowledgeable about a field application whether a model is reasonable and compatible [4]. A common way of validating metamodels has been through face validation using a subject matter expert [5]. This function is more effective than other validation techniques. Interviews in an open planned meeting are guided by the researcher to gain detailed information about a certain topic for research purposes [34]. There are three major types of interviews: structured, semi-structured, and unstructured [35,36]. Structured interviews use common questions for each interviewee, while semi-structured interviews consist of a list of topics to be explored so that the researcher can change the sequence of questions or even add new questions depending on the flow of the discussion. Unstructured interviews mean that the researcher has less control as they only propose a topic and then listen to how the interviewee expresses their views and ideas [34,35]. This paper used structured interviews to validate the developed DBFIM. However, the issue with this kind of validation is identifying and selecting expert participants.

The next phase explains the identification and selection of expert participants.

4.2. Phase B (Figure 5b)*: Conduct Interviews: This Phase Aims to Conduct Interviews to Validate the DBFIM. It Consists of Two Steps: Identification and Selection of Expert Participants; and Conduct Validation*

4.2.1. Identification and Selection of Expert Participants

From the perspective of a qualitative study, the number of participants/experts may be fewer as opposed to quantitative studies [37]. As a result, in order to obtain results that can be relied upon, it is important to highlight the bare minimum sample [38], where existing research shows that the recommended number of participants/experts that could be interviewed in the context of this study ranges between 3 and 20 [39]. That notwithstanding, existing research [40] has also shown that 12 respondents can be treated as a saturation point, this is the motivation that lies behind our study.

Table 1. Metamodel validation techniques.

ID	Validation Technique	Definitions	Critics
1.	Machine-Aided [41]	Metamodel specifications are expressed using a formal language. One possibility would be a metamodeling language based on Boolean predication calculus. Such a calculus can take the form of a supplementary set of constraint expressions written in an appropriate Boolean expression language. Care must be taken to ensure the names of object types and relationships appear correctly in the Boolean expressions.	This technique is used for specific multi-graph machines.
2.	Leave-one-out cross Validation [42]	A method for metamodel verification when additional validation points cannot be afforded. It is a special case of cross-validation. In this approach, each sample point used to fit the model is removed one at a time, after which the model is rebuilt without that sample point, and the difference between the model without the sample point and the actual value at the sample point is computed for all sample points.	Is used to validate lost sensitive data and was developed for mathematical metamodeling purposes.
3.	Multistage Validation [43]	Combination of three chronicled strategies, which are logic, experimentation, and positive financial matters, into a multistage procedure of validation.	This technique was developed for simulation purposes.
4.	Tracing/Traceability [4]	The conduct of particular entities in the model is followed (taken after) through the model to figure out whether the rationale of the model was right and if the essential exactness was acquired.	This technique was introduced to evaluate the logical consistency of metamodels against domain models.
5.	Face Validity [4]	Consults with domain experts that the model was reasonably carried out. This procedure guarantees sensible inputs if it produces sensible outputs (getting some information about the domain by an expert whether the model and/or its behavior is sensible).	This technique was developed to validate the completeness, logicalness, and usefulness of metamodels.
6.	Cross-validation [44]	A strategy to choose a "successful" possibility for real re-enactment by evaluating differences between an anticipated output with every other input	It is a model evaluation technique that can assess the precision of a model without requiring any extra example focuses. It was developed for mathematical metamodeling purposes.
7.	Comparison against other models [4]	Inferred concepts of a created metamodel are validated and the validated model is compared with concepts of other (legitimate) existing comparable "domain models or metamodel".	It used to validate the completeness of the metamodel against domain models.
8.	Bootstrap Approach [32]	A method to test the ampleness of relapse metamodels where the bootstrap appraises the dispersion of any acceptance measurement in arbitrary reproductions with recreated runs.	Bootstrapping is a computationally superior re-sampling technique for simulations. It was developed for simulation modeling purposes.
9.	Formal Ontology [45]	A part of the discipline of ontology in philosophy. It creates general speculations that record parts of reality that are not particular to any field of science, be they in material science or conceptual modeling.	It is used with ontological domains. It focused on theories.
10.	Subjective Validation [46]	A strategy utilized when metamodel information and simulation information do not fulfill the factual presumptions required for target validation.	It is used to validate analog circuit metamodels.
11.	Case Study [47]	A technique to integrate a current formal ontology for information objects with an upper ontology for messages and activities, considering the discourse act hypothesis spoke to consistently utilize UML profiles.	This technique was developed to evaluate the derivation process of metamodels.

Identification and selection of digital forensic experts and modeling experts is not easy [40]. Therefore, three sampling processes were adapted to select experts [41]: handpicked sampling, snowball sampling, and volunteer sampling. Handpicked sampling (specially chosen) processes involves selecting cases that meet criteria. It is the selection of a sample with a particular purpose in mind. The snowball sampling process is often used when working with researchers that are not easily chosen, identified, or accessed. Basically, the process involves building a sample through referrals, beginning by identifying someone from among your researchers who is willing to be in your study, then ask them to identify others who meet the study criteria. The volunteer sampling process simply refers to the process of selecting a sample by asking for volunteers. This may involve putting advertising in the newspaper or going to local organizations such as churches, schools, or community groups.

This paper selected the handpicked sampling process to select experts who had full technical or theoretical experience. This process delivered five (5) digital forensic experts and one (1) modeling expert willing to validate the developed DBFIM. Four experts worked in cybersecurity field in Malaysia, Australia, and the UK. The first expert was a quality manager and digital forensics expert. The second expert was a professor at the School of Science and Technology at Nottingham Trent University. The third expert was an Assistant Professor located at the Department of System and Computer Communication at University Technical Malaysia Melaka (UTEM). The fourth expert was from the Department of Digital Forensics at OSA TECH GROUP. The fifth (5) expert was from the Department of Information System at University Technology Malaysia (UTM). Finally, the sixth expert was a cyber forensics and security researcher at the ECU Security Research Institute at Edith Cowan University, Australia. Table 2 illustrates the participant (experts) profiles.

Table 2. Metamodel validation techniques.

	Digital Forensics Experts
	Expert 1
Designation	Quality manager and digital forensic expert
University/Institute	Cyber Security Malaysia
Department	Digital Forensics Department
Communication Type	Face-to-face
	Expert 2
Designation	Visiting professor at the NTU School of Science and Technology
University/Institute	Nottingham Trent University
Department	School of Science and Technology
Communication Type	Remote communication (LinkedIn and Email)
	Expert 3
Designation	Senior lecturer
University/Institute	University Technology Malaysia Melaka
Department	Department of System and Computer Communication
Communication Type	Face-to-face
	Expert 4
Designation	Managing director at I SEC Academy (M)
University/Institute	I SEC Academy (M) Sdn Bhd
Department	Department of Digital Forensic
Communication Type	Face-to-face
	Expert 5
Designation	Senior Lecturer
University/Institute	UTM
Department	Information System
Communication Type	Face-to-face
	Expert 6
Designation	Cyber forensics and security researcher
University/Institute	Edith Cowan University, Australia
Department	ECU Security research Institute
Communication Type	Remote communication (via Zoom)

4.2.2. Conduct Validation

The validation of the proposed DBFIM will be conducted from two perspectives: the digital forensic perspective and the modeling perspective. The purpose of validation from the digital forensic and modeling perspective is to ensure that all the concepts of the developed DBFIM are relevant to the DBFI field, that all relationships between concepts were defined, and that the logic of the developed DBFIM was achieved [40,42]. Feedback from the expert interviews was used to revise and improve the developed DBFIM. The participant interviews conducted in this study were based on geographic region due to the locations of the participants [43]. Therefore, the face-to-face method was used for participants who resided in a small geographic region, and mobile phones, LinkedIn, Skype, Zoom and email were used for participants who reside in another geographic region. The interview questions of this evaluation were adapted from [40,42].

From the digital forensic perspective, the first interview was conducted with Cybersecurity Malaysia experts. The experts that were selected to evaluate the DBFIM were fully experienced. Interviews with these experts were twice conducted face-to-face. The experts commented on the developed DBFIM as follows:

> "This research is a very good one, and helpful for the lab to understand better about process involves in the DBFI domain. It includes major concepts of DBFI domain in a single model; hence facilitates fast understanding. Definitely, it's useful for a digital forensic lab. On the other methodology per se, it is interesting in finding such a flow can help interpret the forensic investigation process in a much more precise understanding. This model is useful for Cyber Security Malaysia to explain concepts of DBFI to newly hired staff, as well as to the investigation team in Malaysia".

Some valuable modifications were introduced by Expert 1 to improve the developed DBFIM; for example, adding a special relationship between the hashing concept and forensic technique concept due to the hashing concept being a kind of forensic technique concept, and changing the airtight bag concept to the seal concept due to the seal concept being more commonly used amongst investigators. Additionally, this expert added a case objective concept into the artefact analysis class and commented: "Analyst in the lab need to have clear Case Objective (i.e., to extract data from date X to date Y) in order for them to proceed with the analysis". In addition, the expert suggested a types of incident concept under the incident concept in the identification class of the developed DBFIM due to there being some cases where nothing is wrong with the database; it is not being compromised, changed or destroyed, but the investigation team needs to obtain meaningful data from the database. This is more on extracting the right data using SQL statements. For example, a company is running an illegal business, and the database is working fine. In this case, the investigation team needs to obtain, for example, a list of buyers.

Expert 2's interview was held through Email and LinkedIn. This expert was interested in this work and commented "This DBFIM looks very interesting, and a much-needed area to underpin investigation and to set the baseline for the first responder". This expert suggested adding some concepts to improve the developed DBFIM such as severity of case, secure operations center team, and computer security incident response team, where the secure operations center team is defined as "an entity which supervises the security of a company or set of assets" and the computer security incident response team is defined as "The people who engage reported event, or incidents. These people will usually engage in the Digital Forensics Investigation". In addition, this expert suggested changing the "Artefact" concept to "Artifact".

The third interview with (Expert 3) was conducted face-to-face. This expert was interested in this work and commented as follows:

> "The proposed metamodel is able to facilitate the DBFI practitioners on creating the model based on their specific requirements. This could help in reducing the complexity of managing the process forensic investigation especially on acquiring

> and examining the evidence. By having this metamodel, it could reduce the misconception of the terms used during the investigation amongst DBFI users and practitioners in which they're used to the same process of investigation. Also, DBFIM is important to assist forensic examiners to identify and investigate database related incidents in a systematic way that will be acceptable in the court of law. It could help on having a standard term and providing consistency definition on terms used in the investigation. Based on the proposed metamodel, it's comprehensive enough for handling the DBFI".

The fourth interview (Expert 4) was conducted face-to-face at University Technology Malaysia (UTM). The expert was interested in this work and commented that the "Metamodel is helpful and aid investigators understand how forensic investigation should be carried out more appropriately to the crime and result admissibility". However, this expert suggested implementing the DBFIM in a real scenario as "a more proactive approach is required for DBFIM as outlined in figures".

An interview was conducted with Expert 5. This expert works at the Department of Information Systems at the faculty of Computing at University Technology Malaysia (UTM) and has several years of experience with modeling, metamodeling, ontologies, and knowledge management. This participant has published several scientific papers on modeling and ontologies as well as supervised research work at the Ph.D. and master's level related to this field of work. Thus, this participant is seen as an expert in the field.

This expert mentioned that the developed DBFIM had fulfilled the requirements of metamodel structuring/building (e.g., concepts, relationship, and consistency). However, the expert stated that the metamodel of the process is missing and suggested a repository or UML activity diagram to represent the metamodel process. However, the scope of this paper is structuring and organizing DBFI field knowledge. Nonetheless, the expert evaluated DBFIM correctness (syntactically and semantically) and stated:

> "As long as you follow adopted, adjusted and structured methods to establish metamodel from relevant or credible citations. Then it should be ok. The best solution to evaluate the DBFIM correctness, the student must be using application-based and proven syntactic and semantic model by successful prototyping".

The final expert review with (expert 6) was conducted remotely over Zoom. This expert was selected to verify and identify whether the DBFIM was valid in scope and how it was represented. This expert stressed the fact that the DBFIM was valid as long as the scientific approaches were used, and he also suggested the need to adopt the chain of custody in order to increase the chances of safeguarding the infrastructure.

4.2.3. Conduct Validation of Developed DBFIM from a Modelling Perspective

The validation from the modeling perspective concentrates on evaluating the developed DBFIM from the modeling perspective with requirements adopted from [44]: based on the modeling perspective, the authors selected the following aspects:

i. Correctness: Evaluates DBFIM building/structuring.
ii. Relevance: Evaluates the concepts and terminologies relevant to DBFIM. Concepts without relevance may be eliminated or changed.
iii. Economic efficiency: Evaluates the efficiency of DBFIM creation (use and re-use of existing knowledge and solutions).
iv. Clarity: Evaluates the clarity of DBFIM.

As it has clearly been shown, the expert opinions, views, insights, and perceptions about the DBFIM holds very high importance. Given that most of the interview was basically on the relevance and suitability, this enabled the authors to be able to comprehensively create a picture of how suitable the DBFIM is. Ultimately, the DBFIM was validated by all six experts, including their proposed suggestions that were meant to improve the metamodel.

5. Results of Validation

Generally, all experts agreed about the completeness, logicalness, and usefulness of the developed DBFIM. In their opinion, DBFIM addressed all concepts available in the DBFI field in a clear way. The experts agreed that DBFIM was structured and unified in a proper manner.

Expert 1 added the case objective concept to the next version of DBFIM Artefact Analysis Class 3. This expert also added the types of incident concept to the next version of DBFIM Identification Class 1. The experts changed the airtight bag concept to the seal concept in the next version of DBFIM Artefact Analysis Class 3 due to this concept being most commonly most used amongst investigators. In addition, a new relationship between the hashing concept and the forensic technique concept was considered in the next version of the DBFIM.

Expert 2 suggested adding a severity of case concept to the next version of the developed DBFIM; however, this concept is supported by the incident concept. In addition, this expert suggested adding a secure operations center team and a computer security incident response team to DBFIM Identification Class 1. However, these concepts can be instantiated by the investigation Team concept in the DBFIM. In addition, the expert suggested changing the "Artefact" concept to "Artifact". However, the "Artefact" concept has a greater frequency in the DBFI field than the "Artifact" concept.

Expert 4 suggested implementing the developed DBFIM in a real scenario. Hence, the implementation of the developed DBFIM in a real scenario was applied by [20].

Thus, the developed DBFIM was improved by adding two (2) new concepts: types of incident, and case objective, and modifying the airtight bag concept to a seal concept, as well as adding new a relationship between the forensic technique concept and the hashing concept. These modifications changed the first version of developed DBFIM and generated a new version of DBFIM, as shown in Figures 6–9. The next sections discuss the improved DBFIM in detail.

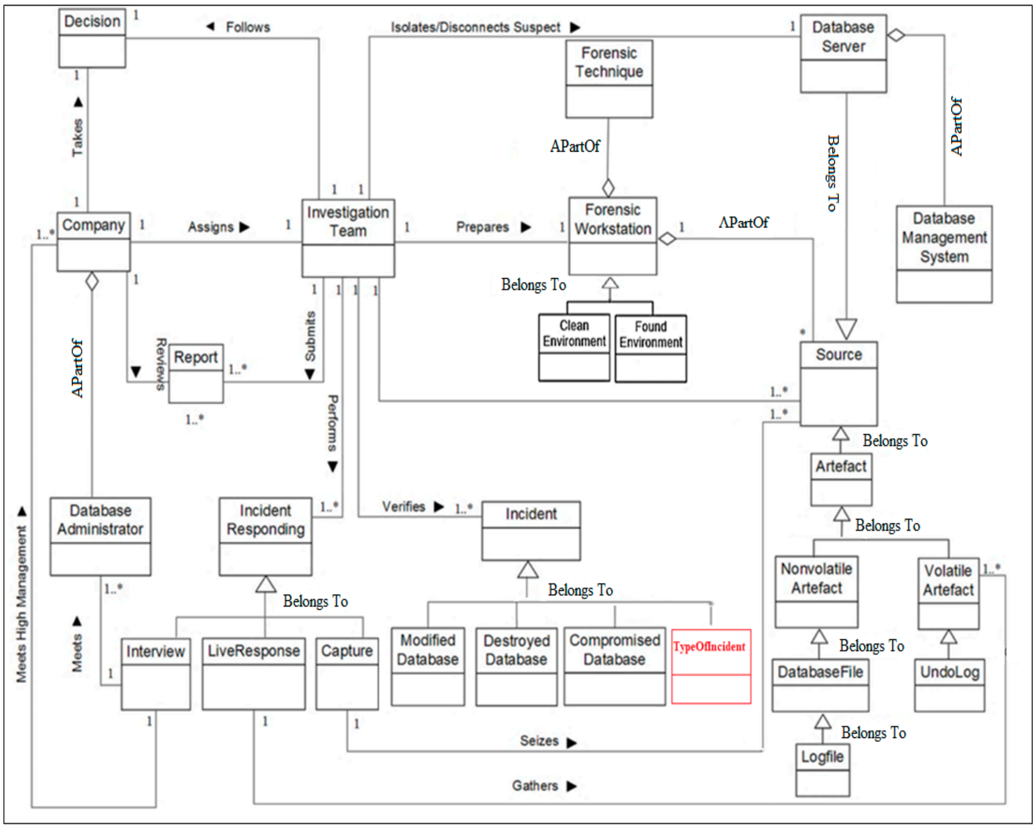

Figure 6. Validated DBFIM Identification Class 1.

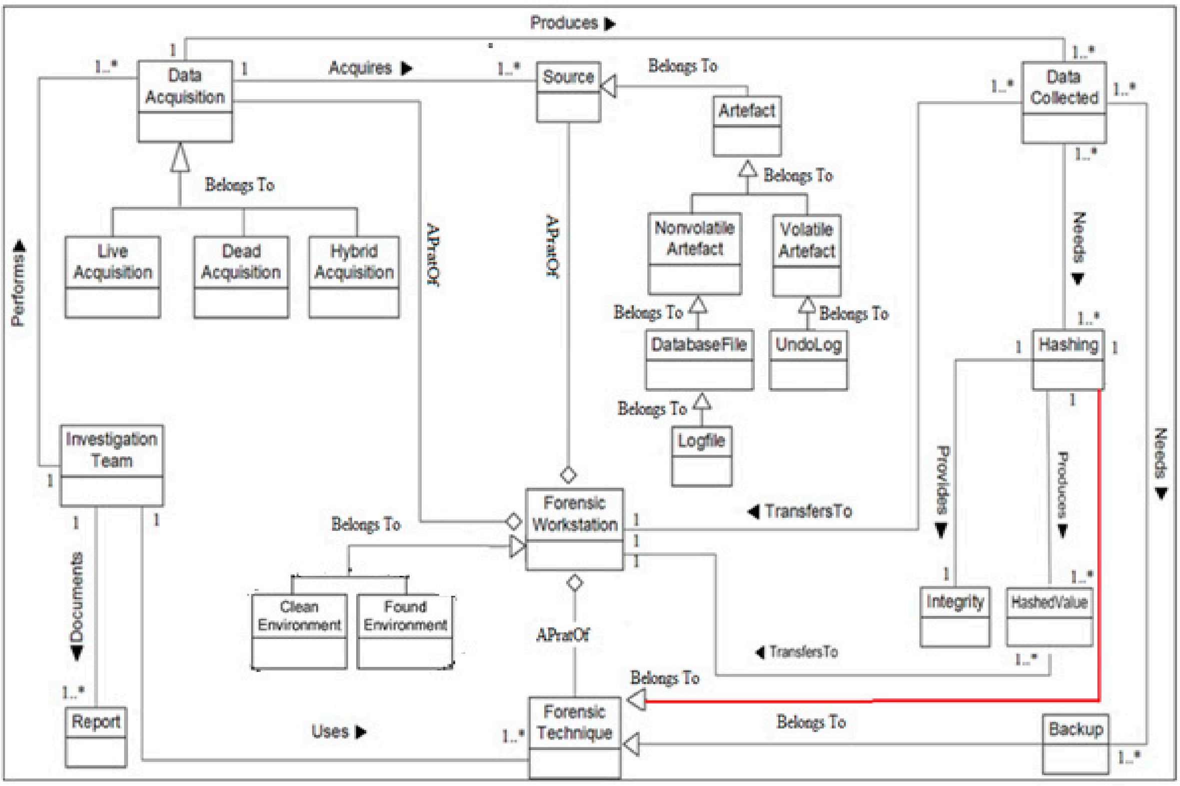

Figure 7. Validated DBFIM Artifact Collection Class 2.

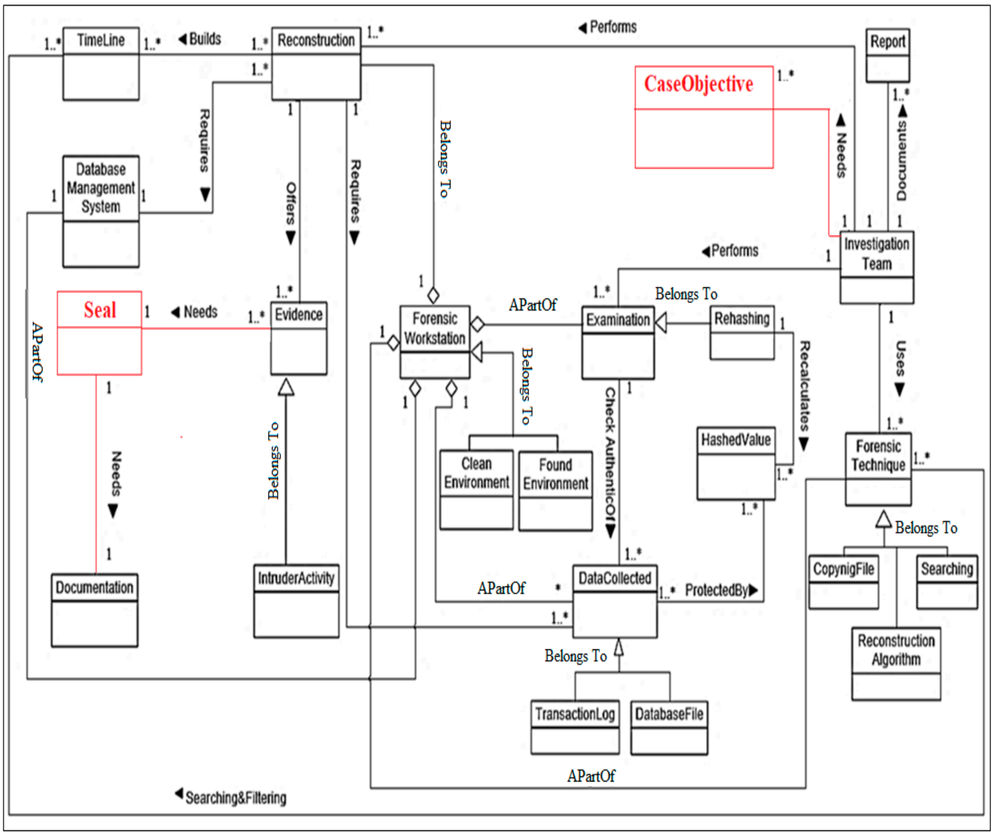

Figure 8. Validated DBFIM Artifact Analysis Class 2.

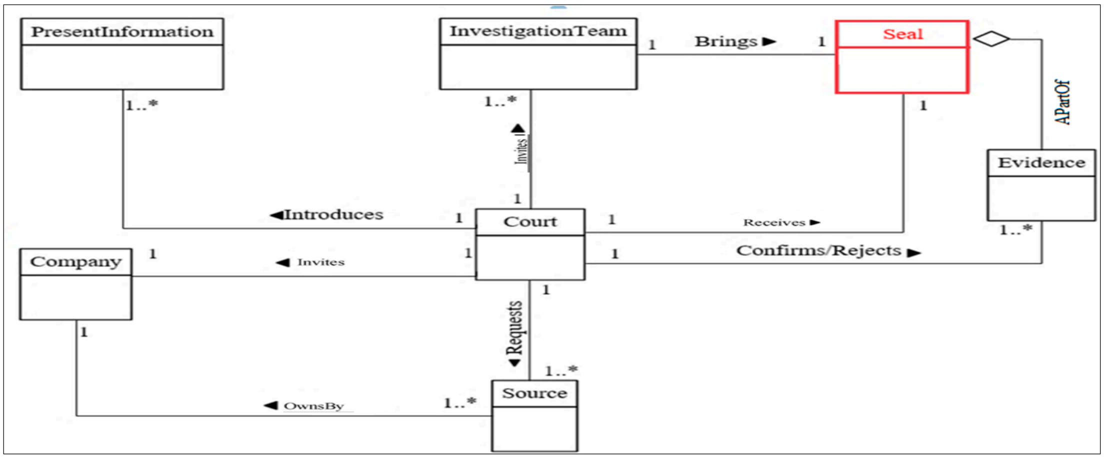

Figure 9. Validated DBFIM Documentation and Presentation Class 4.

5.1. DBFIM Process Class 1: Identification DBFIM

The improved DBFIM process class 1 is illustrated in Figure 6, including six (6) investigative stages: notifying of incident, incident responding, identifying source, and verifying of incident, isolating database server, and preparing investigation environment stage. The first investigative stage is notifying of incident. The DBA of the company notifies higher management staff (e.g., Chief Executive Officer (CEO), Chief Operating Officer (COO), or Chief Security Officer (CSO)) about a database server incident [45]. In this case, the CEO of the company has two choices [46]—either assign an internal/external investigation team to investigate the database server incident or stop the investigation [46]. The investigation team performs the second stage of the identification investigation process, the incident responding stage, to gather incident details such as incident events, parties involved in the investigation, and the number and size of involved databases [46,47].

The investigation team used trusted and cleaned forensic techniques to seize investigation sources [48], gather volatile artifacts [12], and acquire valuable information through staff interviews [49]. The incident responding concept includes three concepts: capture, live response, and interview, as shown in Figure 6. In this way, the investigation team captured investigation sources such as volatile and non-volatile artifacts [12]. In addition, the live response has an association relationship with the volatile artefact concept. Thus, the investigation team gathered valuable volatile data from the volatile artefact concept. The last concept of incident response is the interview concept. The investigation team should conduct interviews with senior company staff such as the DBA and CEO [49]. Basic information such as information accounts, network ports, database servers, users, incident reports, logs, investigation procedures, and policies may be gathered during interviews [49]. Clearly, the incident responding stage allows the investigation team to illustrate the boundaries of an incident and identify investigation sources. The third investigative stage is the identifying source stage, which identifies specific investigation sources [12,46]. An investigation source includes several valuable volatile and non-volatile artifacts that hold valued evidence. Therefore, this stage includes concepts that were seized and captured during the responding stage, such as the source, artefact, volatile artefact, nonvolatile artefact, database file, log file, and undo log concept.

The fourth investigative stage is the verifying of incident stage, which allows the investigation team to check and verify database incidents [46,47]. It consists of nine (9) concepts: investigation team, incident, modified database, destroyed database, compromised database, types of incident, company, report, and decision. Therefore, the investigation team should determine the kind (compromised, destroyed, or modified) [2], nature, and status of an incident. Then the investigation team submits detailed reports about the incident to company management [48]. Company management reviews the reports and makes decisions, after which they decide to either continue with investigation tasks, stop conducting investigation tasks, or to disconnect the database server from the network [12,50]. After verifying and determining the incident, the isolating database server stage is started.

The isolating database server stage is the fifth investigative stage and allows the investigation team to isolate/disconnect a suspect database server from the network to avoid further tampering [7,46]. It consists of three concepts: an investigation team, database server, and database management system. The isolation/disconnection of a suspect database server does not mean a shutdown of that database [12], but does isolate users from the database management system [7,50]. Finally, the investigation team should conduct the preparing investigation environment stage. The preparing investigation environment stage allows the investigation team to prepare the investigation environment and conduct investigation tasks [46]. The investigation environment includes six (6) concepts: investigation team, forensic workstation, clean environment, found environment, forensic technique, and source. The investigation team prepares trusted forensic workstations, which include trusted forensic techniques (forensic tools and methods) and the investigation sources identified in the identifying stage.

5.2. DBFIM Process Class 2: Artifact Collection

The improved DBFIM Process Class 2 illustrated in Figure 7 includes two investigative stages: acquiring data and preserving data stage. The acquiring data stage is used to gather/acquire data from a seized and captured investigation source identified in the identifying source stage [2,12].

It uses some concepts to achieve this mission: investigation team, report, forensic workstation, clean environment, found environment, forensic technique, data acquisition, source, and data collected. The forensic workstation concept includes trusted forensic techniques (forensic tools, and methods) that acquire sources such as volatile artefact and nonvolatile artefact. Investigation teams such as an investigator or examiner are used to achieve data acquisition (live acquisition, dead acquisition, or hybrid acquisition) to acquire volatile and non-volatile data from sources seized and captured during DBFM Process Class 1. The output of this stage is the data collected. The data collected includes the accumulated data throughout the collection process that can be used for the analysis process. These include data relating to database activities, physical log files, and file database servers. Furthermore, these data include evidence of what an intruder did and metadata regarding intruder activities [2,12,47–53]. Therefore, the results of the acquiring stage need to be preserved.

The *preserving data stage* is used to protect the integrity of data collected using the hashing and backup methods [6,7] as well as to prevent any modification of collected data [46,50]. The preserving data stage consists of the data collected, hashing, integrity, backup, hashed value, and forensic workstation concepts. The data collected produced from the acquiring data stage need hashing and backing up to maintain their integrity. Hashing is used to ensure that the database forensics techniques applied to hash the collected data have not changed the data. In addition, it assures the reliability of transferred data between the source and destination [12]. Moreover, the backup concept provides an exact copy of data collected that may be used as a second copy when the original data have been tampered with [6]. Therefore, a copy of the hashed collected data should be transferred to the forensic workstation through secure channels to conduct reconstruction and analysis activities.

5.3. DBFIM Process Class 3: Artifact Analysis

The improved DBFIM Process Class 3 that is illustrated in Figure 8 is used to reconstruct and analyze database events and reveal intruder activities [46]. It includes two investigative stages: examine data collected, and reconstruct data collected.

The *examine data collected stage* is used to ensure that the data collected are authentic and have not been tampered with [9]. It consists of nine (9) concepts: investigation team, report, forensic technique, examination, data collected, forensic workstation, clean environment, found environment, and rehashing. Thus, the first mission of the investigation team is to examine the authenticity of the data collected using these forensic techniques. However, if the collected data have been modified, the investigation team must use clean data collected from the originally collected data. The examination report is issued by the investigation team to document the results of the examination data collected stage.

The *reconstruct data stage* is used to reconstruct timeline events from collected volatile and non-volatile data, which involves retracing past systems, user database activities, past SQL execution histories, stored procedures, and function executions [2,16,54,55]. It consists of nine (9) concepts: forensic workstation, reconstruction, timeline, data collected, investigation team, report, forensic technique, database management system, and evidence. The investigation team, such as the examiner or analyzer, performs a reconstruction process using forensic techniques such as Log Miner [9], forensic algorithms [54].

The reconstruction process uses clean or existing DBMS and data collected to construct a timeline. The timeline is a collection of digital events that have been recognized from the reconstruction process for use during analysis. [47]. Examples of recognized digital events that can be added to an examination timeline are: failed login events, successful login events, and malicious database events [52]. Furthermore, creating a timeline of events can allow an investigator to gain insight into events and involved parties [16]. The timeline concept has an association relationship with the forensic technique, which may be used to search and filter the timeline to provide evidence. Evidence is usually recognized in database files that are recorded on hard drives, storage devices, and media [55]. It is transmitted in binary form and may be relied upon in court [52]. It consists of who, what, when, where, why, and how malicious transactions were carried out [45]. Finally, the investigation team documents the entire reconstruction stage in several reports and for submission to the contracting company and the court.

5.4. DBFIM Process Class 4: Documentation and Presentation

The improved DBFIM Process Class 4 illustrated in Figure 9 is used to document and present investigation stages and submit their results to the court. It consists of seven (7) concepts: investigation team, evidence, court, source, seal, present information, and company. The court invites the investigation team as well as the company to attend the court. The investigation team presents their evidence, and the court receives and checks the authenticity of the evidence and resources. Finally, a final decision is issued by the court.

6. Discussion and Analysis

From the study, the experts were required to give their views on the DBFIM and its suitability. Most of the interview process was explicitly completed with clear questions. All the experts unanimously agreed that the DBFIM was relevant in the context of databases. In addition, all the experts were in agreement that databases represent a very unique and important aspect and it is necessary to verify and validate various approaches in order to be able to identify and recover (artefacts) suspicious activities from a forensic standpoint. In addition, from the conducted interviews, it become apparent that the DBFIM is a baseline for conducting investigations and that it is basically an important incident response asset.

As a result of the interviews with the experts, it has been noted that the DBFIM is important even though most or all of the experts suggested a slight modification to incorporate new concepts to improve the DBFIM; however, a belief was expressed by the experts on the viability of the DBFIM.

Compared to the initial version of the DBFIM, the validated DBFIM is complete, coherent, logical enough, scalable, interoperable, and useful. Three new concepts have been added to the new version of the DBFIM, as shown in Table 3: the types of incident, case objective, and seal concept. Besides making a modification to the metamodel concepts, eight (8) relationships were also added between the concepts. After performing the validations, the DBFIM was further improved.

Table 3. Three new added concepts based on face validity.

DBFIM Process	Concept 1	Concept 2	Modification	Relation Name
Identification	Types of incident	Incident	Add (Specialization)	Belongs to
Artefact Collection	Hashing	Forensic techniques	Add (Specialization)	Belongs to
Artefact Analysis	Case objective	Investigation team	Add (Association)	Needs
	Seal	Evidence	Add (Association)	Needs
	Seal	Documentation	Add (Association)	Needs
Documentation and Presentation	Seal	Investigation team	Add (Association)	Brings
	Seal	Evidence	Add (Specialization)	A part of
	Seal	Court	Add (Association)	Receives

The findings that were realized as result of face validity review show that the selected experts viewed the metamodel at an important aspect that could have an influence in the field of database forensics. It is worth mentioning that the suggestions of the experts were duly considered in improving the DBFIM, producing a validated DBFIM that is logical enough and that can be accepted within the forensic community.

7. Conclusions

This paper concentrated on the validation stage of DBFIM to prove the completeness, usefulness, and logicalness of the developed DBFIM. For this purpose, face validity has been used. The face validity method is a common way of validating metamodels by asking individuals knowledgeable about the domain application whether the metamodel is reasonable and compatible using a subject matter expert. Thus, six experts were selected to validate the proposed DBFIM. From the expert review, the proposed DBFIM was complete, coherent, logical, scalable, interoperable, and useful for the DBFI field. The future work will include implementing the DBFIM in the real scenarios to ensure the applicability of the DBFIM on the real database crimes.

Author Contributions: Conceptualization: A.A.-D., S.R., S.H.O., R.A.I., V.R.K.; Investigation: A.A.-D., S.R., S.H.O., R.A.I., V.R.K.; Writing—original draft preparation: A.A.-D., S.R., S.H.O., R.A.I., V.R.K.; Supervision: S.R., S.H.O.; Review and Editing: A.A.-D., S.R., S.H.O., R.A.I., V.R.K.; Project administration: S.R., S.H.O.; Editing and Proofs: A.A.-D., S.R., S.H.O., R.A.I., V.R.K.; Correspondence: V.R.K. All authors have read and agreed to the published version of the manuscript.

Funding: Open Access Funding of this research has been provided by Malmö University, Nordenskiöldsgatan 1, 21119, Malmö, Sweden.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Al-Dhaqm, A.M.R.; Othman, S.H.; Razak, S.A.; Ngadi, A. Towards adapting metamodelling technique for database forensics investigation domain. In Proceedings of the 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, Malaysia, 26–27 August 2014; pp. 322–327.
2. Fasan, O.M.; Olivier, M.S. On Dimensions of Reconstruction in Database Forensics. In Proceedings of the Workshop on Digital Forensics & Incident Analysis(WDFIA 2012), Crete, Greece, 6–8 June 2012; pp. 97–106.
3. Al-dhaqm, A.; Razak, S.; Othman, S.H.; Ngadi, A.; Ahmed, M.N.; Mohammed, A.A. Development and validation of a Database Forensic Metamodel (DBFM). *PLoS ONE* **2017**, *12*, e0170793. [CrossRef] [PubMed]
4. Sargent, R.G. Verification and validation of simulation models. In Proceedings of the 37th Conference on Winter Simulation, Baltimore, MD, USA, 5–8 December 2010; pp. 130–143.
5. Goerger, S.R. *Validating Computational Human Behavior Models: Consistency and Accuracy Issues*; Naval Postgraduate School: Monterey, CA, USA, 2004.
6. Olivier, M.S. On metadata context in database forensics. *Digit. Investig.* **2009**, *5*, 115–123. [CrossRef]

7. Wong, D.; Edwards, K. System and Method for Investigating a Data Operation Performed on a Database. U.S. Patent Application 10/879,466, 29 December 2005.
8. Wright, P.M. *Oracle Database Forensics Using Logminer*; Global Information Assurance Certification Paper; SANS Institute: Bethesda, MD, USA, 2005.
9. Litchfield, D. *Oracle Forensics Part 1: Dissecting the Redo Logs*; NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd.: Sutton, UK, 2007.
10. Litchfield, D. *Oracle Forensics Part 2: Locating Dropped Objects*; NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd.: Sutton, UK, 2007.
11. Litchfield, D. *Oracle Forensics: Part 3: Isolating Evidence of Attacks Against the Authentication Mechanism*; Next Generation Security Software Ltd.: Sutton, UK, 2007.
12. Litchfield, D. *Oracle Forensics Part 4: Live Response*; Next Generation Security Software Ltd.: Sutton, UK, 2007.
13. Litchfield, D. *Oracle Forensics Part 5: Finding Evidence of Data Theft in the Absence of Auditing*; Next Generation Security Software Ltd.: Sutton, UK, 2007.
14. Litchfield, D. *Oracle Forensics Part 6: Examining Undo Segments, Flashback and the Oracle Recycle Bin*; Next Generation Security Software Ltd.: Sutton, UK, 2007.
15. Litchfield, D. *Oracle Forensics Part 7: Using the Oracle System Change Number in Forensic Investigations*; NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd.: Sutton, UK, 2008.
16. Wagner, J.; Rasin, A.; Grier, J. Database forensic analysis through internal structure carving. *Digit. Investig.* **2015**, *14*, S106–S115. [CrossRef]
17. Ogutu, J.O. A Methodology to Test the Richness of Forensic Evidence of Database Storage Engine: Analysis of MySQL Update Operation in InnoDB and MyISAM Storage Engines. Ph.D. Thesis, University of Nairobi, Nairobi, Kenya, 2016.
18. Wagner, J.; Rasin, A.; Malik, T.; Hart, K.; Jehle, H.; Grier, J. Database Forensic Analysis with DBCarver. In Proceedings of the CIDR 2017, 8th Biennial Conference on Innovative Data Systems Research, Chaminade, CA, USA, 8–11 January 2017.
19. Al-Dhaqm, A.; Razak, S.; Othman, S.H.; Choo, K.-K.R.; Glisson, W.B.; Ali, A.; Abrar, M. CDBFIP: Common Database Forensic Investigation Processes for Internet of Things. *IEEE Access* **2017**, *5*, 24401–2441621. [CrossRef]
20. Al-Dhaqm, A.; Razak, S.; Othman, S.H. Model Derivation System to Manage Database Forensic Investigation Domain Knowledge. In Proceedings of the 2018 IEEE Conference on Application, Information and Network Security (AINS), Langkawi, Malaysia, 21–22 November 2018.
21. Hungwe, T.; Venter, H.S.; Kebande, V.R. Scenario-Based Digital Forensic Investigation of Compromised MySQL Database. In Proceedings of the 2019 IST-Africa Week Conference (IST-Africa), Nairobi, Kenya, 8–10 May 2019.
22. Khanuja, H.K.; Adane, D. To Monitor and Detect Suspicious Transactions in a Financial Transaction System Through Database Forensic Audit and Rule-Based Outlier Detection Model. In *Organizational Auditing and Assurance in the Digital Age*; IGI Global: Hershey, PA, USA, 2019; pp. 224–255.
23. Al-Dhaqm, A.; Abd Razak, S.; Dampier, D.A.; Choo, K.-K.R.; Siddique, K.; Ikuesan, R.A.; Alqarni, A.; Kebande, V.R. Categorization and organization of database forensic investigation processes. *IEEE Access* **2020**, *8*, 112846–112858. [CrossRef]
24. Al-Dhaqm, A.; Abd Razak, S.; Siddique, K.; Ikuesan, R.A.; Kebande, V.R. Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. *IEEE Access* **2020**, *8*, 145018–145032. [CrossRef]
25. Al-Dhaqm, A.; Abd Razak, S.; Othman, S.H.; Ali, A.; Ghaleb, F.A.; Rosman, A.S.; Marni, N. Database Forensic Investigation Process Models: A Review. *IEEE Access* **2020**, *8*, 48477–48490. [CrossRef]
26. Zhang, Y.; Li, B.; Sun, Y. Android Encryption Database Forensic Analysis Based on Static Analysis. In Proceedings of the 4th International Conference on Computer Science and Application Engineering, New York, NY, USA, 20–22 October 2020; pp. 1–9.
27. Hu, P.; Ning, H.; Qiu, T.; Song, H.; Wang, Y.; Yao, X. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet Things J.* **2017**, *4*, 1143–1155. [CrossRef]
28. Sargent, R.G. Verification and validation of simulation models. In Proceedings of the 2010 Winter Simulation Conference, Baltimore, MD, USA, 5–8 December 2010; pp. 166–183.
29. De Kok, D. Feature selection for fluency ranking. In Proceedings of the 6th International Natural Language Generation Conference, Dublin, Ireland, 7–9 July 2010; pp. 155–163.
30. Bermell-Garcia, P. A Metamodel to Annotate Knowledge Based Engineering Codes as Enterprise Knowledge Resources. Ph.D. Thesis, Cranfield University, Cranfield, UK, 2007.
31. Shirvani, F. Selection and Application of MBSE Methodology and Tools to Understand and Bring Greater Transparency to the Contracting of Large Infrastructure Projects. Ph.D. Thesis, University of Wollongong, Keiraville, Austrilia, 2016.
32. Kleijnen, J.P.; Deflandre, D. Validation of regression metamodels in simulation: Bootstrap approach. *Eur. J. Oper. Res.* **2006**, *170*, 120–131. [CrossRef]
33. Kleijnen, J.P. Kriging metamodeling in simulation: A review. *Eur. J. Oper. Res.* **2009**, *192*, 707–716. [CrossRef]
34. Oates, B. *Researching Information Systems and Computing*; SAGE: Thousand Oaks, CA, USA, 2006.
35. Hancock, M.; Herbert, R.D.; Maher, C.G. A guide to interpretation of studies investigating subgroups of responders to physical therapy interventions. *Phys. Ther.* **2009**, *89*, 698–704. [CrossRef] [PubMed]
36. Robson, C. *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*; Blackwell Oxford: Oxford, UK, 2002; Volume 2.

37. Hancock, B.; Ockleford, E.; Windridge, K. *An Introduction to Qualitative Research: Trent Focus Group Nottingham*; Trent Focus: Nottingham, UK, 1998.
38. Banerjee, A.; Chitnis, U.; Jadhav, S.; Bhawalkar, J.; Chaudhury, S. Hypothesis testing, type I and type II errors. *Ind. Psychiatry J.* **2009**, *18*, 127. [CrossRef] [PubMed]
39. Grant, J.S.; Davis, L.L. Selection and use of content experts for instrument development. *Res. Nurs. Health* **1997**, *20*, 269–274. [CrossRef]
40. Hauksson, H.; Johannesson, P. Metamodeling for Business Model Design: Facilitating development and communication of Business Model Canvas (BMC) models with an OMG standards-based metamodel. Master's Thesis, KTH Royal Institute, Stockholm, Sweden, 2013.
41. O'Leary, Z. *The Essential Guide to doing Research*; Sage: Thousand Oaks, CA, USA, 2004.
42. Othman, S.H. Development of Metamodel for Information Security Risk Management. Ph.D. Thesis, Universiti Teknologi Malaysia, Johor, Malaysia, 2013.
43. Bandara, W.; Indulska, M.; Chong, S.; Sadiq, S. Major issues in business process management: An expert perspective. In Proceedings of the 15th European Conference on Information Systems, St Gallen, Switzerland, 7–9 June 2007.
44. Becker, J.; Rosemann, M.; Von Uthmann, C. Guidelines of business process modeling. In *Business Process Management*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 30–49.
45. Frühwirt, P.; Kieseberg, P.; Krombholz, K.; Weippl, E. Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations. *Digit. Investig.* **2014**, *11*, 336–348. [CrossRef]
46. Fowler, K. *SQL Server Forenisc Analysis*; Pearson Education: London, UK, 2008.
47. Fowler, K.; Gold, G.; MCSD, M. A real world scenario of a SQL Server 2005 database forensics investigation. In *Information Security Reading Room Paper*; SANS Institute: Bethesda, MD, USA, 2007.
48. Choi, J.; Choi, K.; Lee, S. Evidence Investigation Methodologies for Detecting Financial Fraud Based on Forensic Accounting. In Proceedings of the CSA'09, 2nd International Conference on Computer Science and its Applications, Jeju Island, Korea, 10–12 December 2009; pp. 1–6.
49. Son, N.; Lee, K.-G.; Jeon, S.; Chung, H.; Lee, S.; Lee, C. The method of database server detection and investigation in the enterprise environment. In Proceedings of the FTRA International Conference on Secure and Trust Computing, Data Management, and Application, Crete, Greece, 28–30 June 2011; pp. 164–171.
50. Susaimanickam, R. A Workflow to Support Forensic Database Analysis. Ph.D. Thesis, Murdoch University, Murdoch, Australia, 2012.
51. Lee, D.; Choi, J.; Lee, S. Database forensic investigation based on table relationship analysis techniques. In Proceedings of the 2009 2nd International Conference on Computer Science and Its Applications, CSA 2009, Jeju Island, Korea, 10–12 December 2009.
52. Khanuja, H.K.; Adane, D. A framework for database forensic analysis. *Comput. Sci. Eng. Int. J. (CSEIJ)* **2012**, *2*, 27–41. [CrossRef]
53. Adedayo, O.M.; Olivier, M.S. Ideal Log Setting for Database Forensics Reconstruction. *Digit. Investig.* **2015**, *12*, 27–40. [CrossRef]
54. Pavlou, K.E.; Snodgrass, R.T. Forensic analysis of database tampering. *ACM Trans. Database Syst. (TODS)* **2008**, *33*, 30. [CrossRef]
55. Tripathi, S.; Meshram, B.B. Digital Evidence for Database Tamper Detection. *J. Inf. Secur.* **2012**, *3*, 9. [CrossRef]