This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Digital Forensics Subdomains: The State of the art and Future Directions

Arafat Al-Dhaqm[1,2], Richard A. Ikuesan[3], Victor R. Kebande[4], Shukor Razak[1], George Grispos[5], Kim-Kwang Raymond Choo[6], Bander Ali Saleh Al-rimy[1], AbdulRahman A. Alsewari[7]

[1] School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia (UTM), Johor, Malaysia (email:mrarafat1@utm.my)
[2] Department of Computer Science, Aden Community College (ACC), Aden, Yemen
[3] Department of Cybersecurity and Networking, School of Information Technology, Community College of Qatar, Doha, Qatar
[4] Department of Computer Science & Media Technology, Malmö University, Sweden (victor.kebande@mau.se)
[5]School of Interdisciplinary Informatics, University of Nebraska at Omaha, Omaha, NE, 68182, USA (email: ggrispos@unomaha.edu)
[6] Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, USA (email: raymond.choo@fulbrightmail.org)
[7]IBM Centre of Excellence, Faculty of Computing, Universiti Malaysia Pahang, Pahang, 26600, Malaysia

Corresponding authors: Richard A. Ikuesan (rikuesan@hotmail.com) , Victor R. Kebande (victor.kebande@mau.se), Bander Ali Saleh Al-rimy (bander@utm.my)
This work was supported by the Open Access Funding provided by the Qatar National Library

ABSTRACT For reliable and relevant scientific evidence to be admitted in a court of law, it is important to apply digital forensic investigation techniques to corroborate a suspected potential security incident. Mainly, traditional digital forensics techniques have focused on computer desktops and servers. However, recent advances in digital media and platforms have seen an increased need for the application of digital forensic investigation techniques to other subdomains including small and mobile devices, databases, networks, cloud-based platforms, and the Internet of Things (IoT). To assist forensic investigators, conduct investigations within these subdomains, academic researchers have attempted to develop a number of investigative processes. However, many of these processes are domain-specific or describe domain-specific investigative tools. Hence, we hypothesize that the literature is littered with potentially overlapping and contradicting investigative process for conducting investigations within these subdomains. To investigate this hypothesis, a digital forensic model-orientated Systematic Literature Review (SLR) within the above digital forensic subdomains was undertaken. The purpose of the SLR was to identify the different and heterogeneous practices that have emerged within the specific subdomains. A key finding from the SLR is that there is a potential information overload and a high-degree of ambiguity among investigative processes in the above subdomains. The outcome of this study proposes a high-level abstract metamodel called The Digital Forensic Metamodel (DFM), which combines common processes, activities, techniques, and tasks for the above subdomains.

INDEX TERMS Digital forensics, Database forensics, Mobile forensic, Network forensics, IoT forensics, Digital Forensic Metamodel

I. INTRODUCTION

The implementation of cybersecurity systems and processes is often inadequate to ensure the Confidentiality, Integrity Availability, and Authenticity (CIAA) of information. As a result, digital forensic processes and techniques are often required to investigate potential security incidents and digital crimes if the CIAA is violated. In 2001, a group of researchers defined digital forensics as "*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources to facilitate or further the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations*" [1]. Since this definition was proposed, various investigative frameworks and process models have also been developed that have a focus on digital forensics. Previously, many of these models were designed to facilitate the investigation of traditional computer systems, such as desktops and servers. However, digital forensics and investigations have transcended the classical desktop-server potential evidence retriever process [2]. The emergence of security incidents across these digital components such as databases, computer networks, mobile devices, and the Internet of Things (IoT), the cloud, and across the network

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

design edges has necessitated the need to develop digital forensic models, processes, and techniques suitable for their respective environments.

As a result, the digital forensic community is gradually experiencing exponential growth of research outputs that are dedicated to the development of tools and processes to recover different types of evidence and artifacts from these subdomains. Given that most of these tools and process models are contextual and issue-specific, there exists a propensity of a high-level domain problem, which is often associated with standardization. At its core, the lack of standardization for any given domain presents grounds for ambiguity, unregularized process, and context-dependent analysis. Taken together, these consequential elements are a primary source of evidence dismissal during litigation. The lack of a uniform approach to corroborate any fact during a digital investigation can therefore lead to evidence inadmissibility. Furthermore, a lack of standardization could also introduce an investigative dilemma on the selection of appropriate processes and techniques for a given investigative procedure, in a specific subdomain.

This study sought to provide substantial insights into the lack of standardization by reviewing existing literature to identify the extent to which tools and techniques have been proposed by the various subdomain communities. More specifically, this study aims to highlight the different and heterogeneous practices that have emerged within the subdomains of mobile device forensics, network forensics, database forensics, and IoT forensics. A depiction of the various subdomains of digital forensics is further summarized in Figure 1.

Eight interconnected subdomains are identified in Figure 1. Whilst subdomains such as network forensics, multimedia forensics, and small device forensics can be defined as a compound subdomain, other subdomains can be defined as simple subdomains. As further highlighted in Figure 1, the scope of digital forensics has attempted to integrate forensic readiness as a component within the core components of digital forensics. Forensic readiness also referred to as proactive forensics, is a business-continuity concept (largely influenced by the requirements from different stakeholders) which is gaining wider adoption in each subdomain. The integration of readiness into these subdomains has been defined as a potential avenue for the development of relevant digital forensic models and frameworks. However, as with any forensic discipline, the respective stakeholders are also required to work within a scientifically verifiable spectrum, to aid evidence admissibility in any judicial proceedings. Moreover, these processes are often required to follow a generally acceptable pre-defined or stipulated guidelines, as substantiated in the Daubert and Frye Judicial proceedings that pertains to forensic evidence admissibility.

As a step in this direction, this study attempts to explicate the various methodologies and stipulated guidelines in the subdomains of digital forensics, to articulate the convergent and divergent (where applicable) towards a unified generally acceptable guideline. Two supportive, yet distinctive subdomains; proactive forensics and behavioral biometrics are further considered in this study, as is shown in Figure 1.

Studies on the proactive forensics approach have mainly explored forensic readiness within the context of the ISO/IEC 27043:2015 standard [3]–[9].

Proactive approaches towards enhancing digital forensics suggest that measures can be implemented within the system under consideration in such a way that relevant and potentially useful pieces of evidence can be collected in a forensically sound manner prior to the occurrence of a digital incident. This approach can therefore provide a complementary source of digital artefacts for volatile environments or instances where potentially useful digital artefacts would otherwise be unavailable [10], [11].

On the other hand, behavioral biometrics provides a complementary approach to generate behavioral attributes of digital artefacts in a manner which can be forensically preserved for digital investigation. Behavioral biometrics is the process of identifying, extracting, and presenting soft attributes of the user of a digital object(s), in such a way that an action or a series of actions can be attributed to a user with minimal ambiguity. This approach is gradually gaining wider adoption within the digital forensic subdomains, as highlighted in recent studies [12]–[17]. Given that behavioral biometrics is an integrated component within any subdomain, the potential of harnessing such a component for digital forensics further makes it a potentially useful component in the DF domain. Components of behavioral biometrics within the network domain include user-initiated network packet requests, network traffic usage patterns, as well as network burstiness characteristics [18]. Similarly, the behavioral composition of usage patterns can be extracted for computer forensics, mobile phone forensics, database forensics, software forensics (especially in identifying unique coding sequence and fingerprint of a software developer), as well as multimedia forensics.

To the best of the authors' knowledge, this is the first study to provide such a comprehensive review of the subdomains within the DF domain, while considering the other complementary components. Furthermore, the methodology utilized in this study presents an alternative approach to conducting a systematic literature review. An integrated forensic model is further presented as an approach towards developing a harmonized forensic model for the DF domain that is well suited to address the aspect of standardization. This proposition is particularly relevant in the development of a domain-based knowledge base platform for digital forensics subdomains. A DF Knowledge Base (DF-KB) has been asserted as a potential approach towards a common DF lexicon and domain management [19]. The next section details the methodology used to develop the review process.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

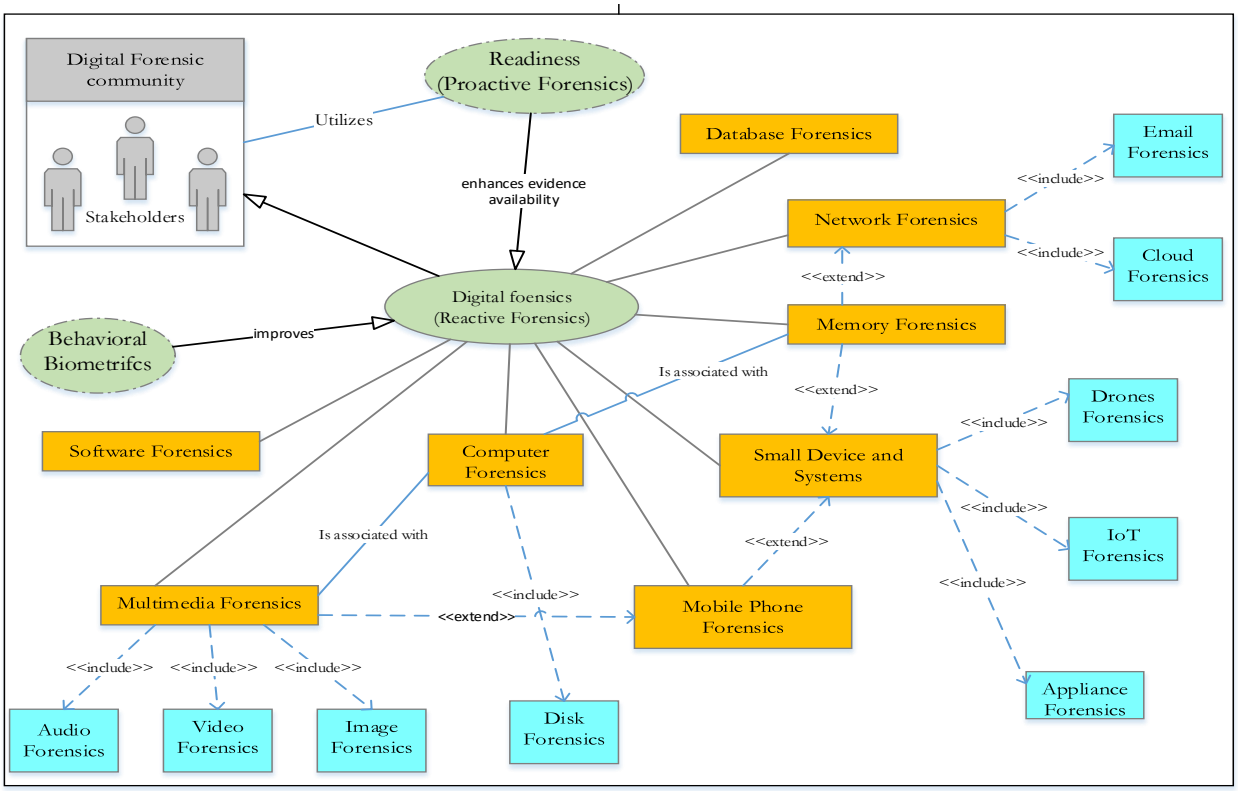

Figure 1. **Illustration of the various subdomains of digital forensics**

II. RESEARCH METHODOLOGY

The purpose of this research is to highlight the different and heterogeneous practices that have emerged within the digital forensics' subdomains. A Systematic Literature Review (SLR) has been conducted as per the guidelines described by [20], as shown in Figure 2. The adapted approach follows a waterfall methodology, with the following steps 1) specification of the research questions; 2) development of the review protocol; 3) conducting the review using the protocol to identify relevant research; 4) Selection of the appropriate repositories; 5) synthesizing the results, and 6) writing the review findings. To further clarify the content and direction of the review, the following research questions are used as a guide to the SLR process.

1. What approaches have been proposed in the existing literature that can guide the forensic investigation of databases, small devices and systems, computer networks, the internet of things, device memory, and multimedia components?
2. What are the limitations (if any) of the proposed approaches in the literature that are used to conduct a digital forensic investigation of the aforementioned subdomains?
3. What challenges (if any) are associated with conducting digital forensic investigations of the above-mentioned subdomains?

To identify relevant literature, searches were undertaken using Web of Science, SpringerLink, IEEE Xplore, Scopus, and ACM Digital Library. These searches were undertaken using the following keywords:

1 "Database Forensics" OR ("Database" AND "digital forensics")

2 "Network Forensics" OR ("Network" AND "digital forensics")

3 "Mobile Forensics" OR ("Mobile" AND "digital forensics")

4 "IoT Forensics" OR ("IoT" AND "digital forensics")

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

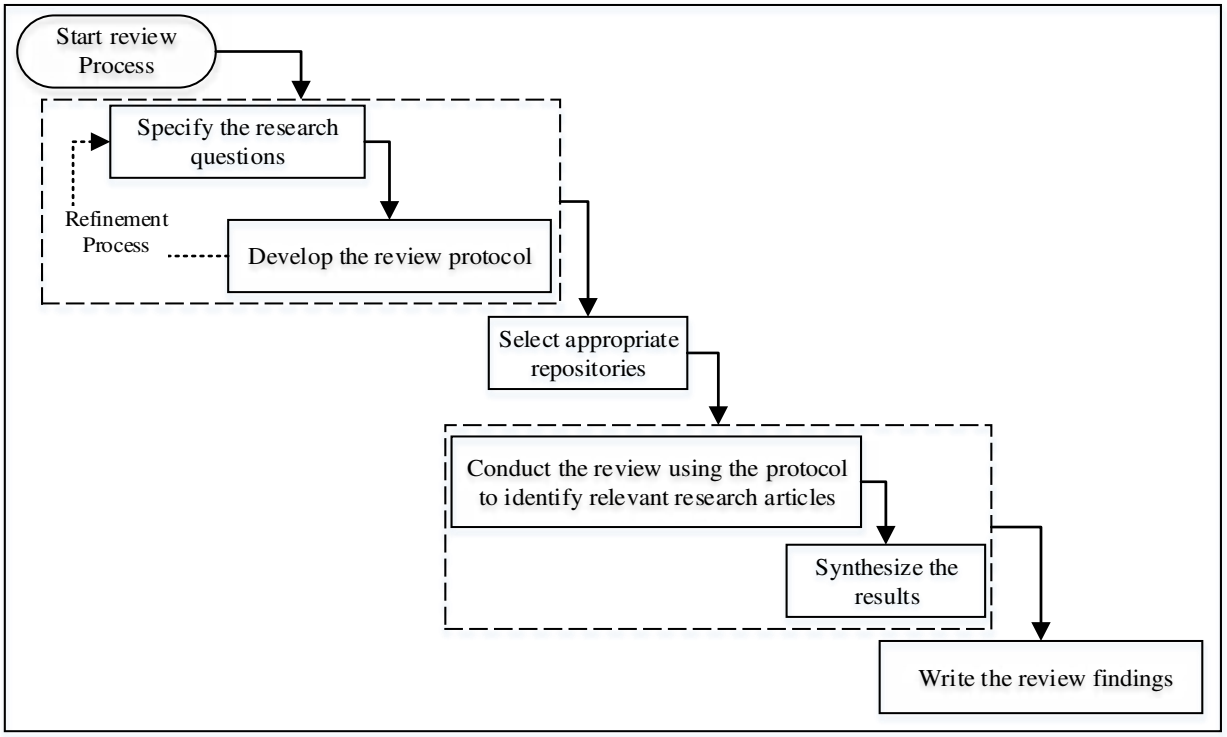

Figure 2. **Adapted Review Approach**

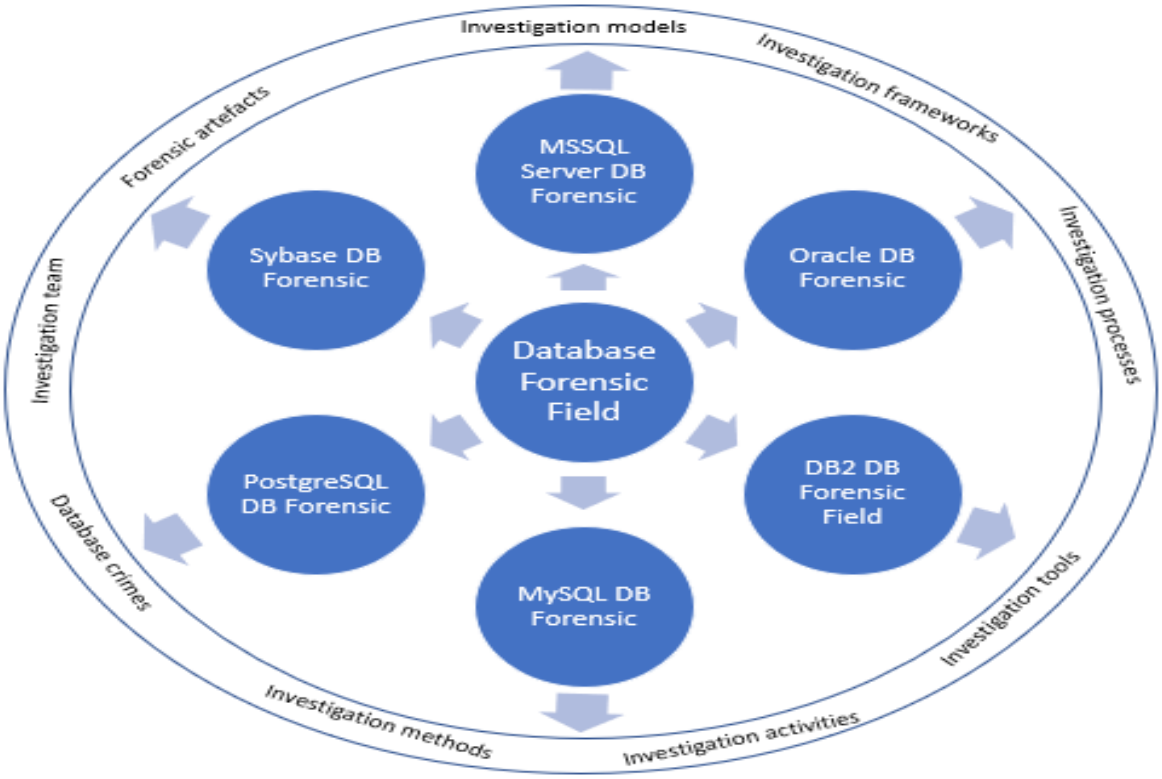

Figure 3. **Database Forensic field**

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

The search employed in this study was specifically confined between the years 2000 and 05/2021. Additionally, the publications included in the search consisted of journal articles, conference papers, dissertations, books, and book chapters. All other publications were excluded from the search process, as such were deemed inappropriate as an academic resource. Furthermore, if a paper was found to be related to the study, its references were examined to identify further papers of interest. Hence, Google Scholar was used to locate further papers of interest in the study. The results from these searches were then analyzed to remove duplicated publications.

This resulted in a dataset of 11,993 publications. These publications were then reviewed, by reading the abstract, introduction, and conclusions sections to categorize the papers as "related" or "non-related" to forensically investigating one of the subdomains. This resulted in a second data set of 240 publications. Finally, the papers were examined and included in the study if they satisfied one of the following inclusion criteria:

- the publication was related to the forensic study of one of the subdomains.
- the publication focused on investigating individual aspects of a subdomain, or
- the publication focused on investigating underlying technologies that make up a subdomain.

The outcome of this final filtering resulted in a data set of 240 publications. These publications were then studied to identify the activities, processes, procedures, and challenges related to conducting forensic investigations of the four subdomains.

III. DATABASE FORENSICS

Database forensics is a significant field used to reveal database crimes. Numerous forensic investigation models, frameworks, processes, and tools have been proposed in the literature for database forensics as illustrated in Figure 3. However, these models are specific because of the complicatedness and multidimensionality of the Database Management Systems (DBMSs). This branch is still in need of more research into all types of database systems. This assertation is further echoed in several recent findings [21], [22], where the logic of harmonized database forensic model conceptualized.

In [23]–[27], the authors assert that database forensics models might fail when applied to the investigation of database systems. This failure can be attributed to the diversity of database management systems (DBMS) and the multidimensionality of database systems. Besides, database forensics also focuses on one dimension (file system), which is primarily hinged on identifying, gathering, handling, storing, giving responses to incidents, and training [23]. Though, in some cases, it may be difficult to trace database incidents without a proportionate degree of cooperation amongst digital investigators regarding the analysis of the database [23]. Furthermore, database forensics practices do not cover the transactional database features. The challenge of multidimensionality and diversity of DBMS have made it difficult to develop a standardized approach for database forensics. Thus, the currently-used digital forensics models fail to cover the entire spectrum of database system concepts [28]. In general, database forensics research uncovered in the literature tends to focus on retrieving database contents along with metadata which suggests accomplishment of various tasks regarding document evidence versus database incidents [29], [30]. A summary of the reviewed literature is presented in Table 1.

To elaborate on some instances, it should be noted that the authors [31] introduced an investigation process model that performs certain tasks to find relevant information on operations conducted on Oracle Database concepts. In the solution the study suggests four research processes: canceling the database operation, collecting data, reconstructing a database, and fixing the integrity of the database. In addition, [21] developed the Log Miner tool for the Oracle database for purposes of reconstructing the actions when the auditing features are turned off.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

Table 1. Database Forensic Models

Year	Database Forensic Investigation Models	Dimensions of Database Forensics			Type of Model														Types of DBMSs					NIST standard forensic procedures				Digital Forensics Readiness		Decreases Heterogeneity and Ambiguity	
		Compromised DB	Destroyed DB	Modified DB	Technical	Conceptual	Oracle DB	MSSQL DB	MySQL DB	Sybase DB	DB2 DB	PostgreSQL DB	SQLite DB	Apache Derby	Firebird	Maria DB	Greenplum	General	Preservation	Acquisitions	Analysis	Reporting	Adopt pre-incident guidance	Provides Mean of Assessing for forensics readiness	Offer Interoperability	Offer Unified Platform
2004	[33]	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2004	[31]	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2004	[32]	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
2007	[34]	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2007	[35]	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2007	[36]	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2007	[37]	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2007	[38]	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2007	[39]	✓	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2007	[40]	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2007	[41]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2008	[42]	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
2008	[43]	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2006	[44]	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2009	[30]	✓	✗	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2009	[45]	✓	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2010	[46]	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2011	[47]	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2011	[48]	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2011	[49]	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2011	[50]	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2012	[51]	✓	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2012	[29]	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
2012	[26]	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
2012	[52]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2012	[53]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2012	[54]	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2012	[55]	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2012	[56]	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[57]	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[58]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[59]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[60]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[61]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[62]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[63]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[64]	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2013	[65]	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2014	[66]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2014	[67]	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2014	[68]	✓	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2014	[25]	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2014	[69]	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2015	[70]	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2014	[71]	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

2015	[72]	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
2015	[73]	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
2016	[74]	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
2016	[75]	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
2016	[23]	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
2017	[76]	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗
2017	[77]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	✓
2017	[78]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
2018	[79]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
2019	[80]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
2020	[22]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
2020	[21]	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗
2021	[81]	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗

Several forensic investigation models have been proposed that have a focus on Oracle Database. For example, the first model showed the way an examiner can utilize an Oracle log file to reveal attacker events [37]. The binary format for the redo logs, which indicates where the evidence can be found, was examined. This examination also determined the way evidence can be integrated into an events timeline. In addition, the study found out the way an attacker attempts to cover their tracks based on a failed attack and also the way to spot it.

The second investigation of the forensic model suggests the way to recover evidence (in the case of Oracle objects) that have been already deleted [38]. It helps investigators to indirectly recover evidence from the data files of the server that has been compromised. Moreover, an entity with malicious intent can also drop the objects. However, using the Oracle DB Views and Tables, an investigator can locate the dropped objects such as OBJ$, IDL_UB1$, SOURCE$, IDL_CHAR$, and RECYCLEBIN$ tables.

A forensic model designed to capture the evidence of attacks against authentication mechanism which leverages the Listener's log file and the audit trail is presented in [82]. This log file contains details of the connections to the database server, such as the name of the Service Identifier (SID), the Internet Protocol (IP) address, and the instance name. On the other hand, the audit trail typically contains details of successful and unsuccessful login and logoff attempts. As a result, examiners can collect evidence against the authentication mechanism from the Listener's log file and the audit trail. This is predicated on the assumption that the audit trail is enabled in the respective DB.

The fourth investigation forensic model was introduced by [83]. This model concerns the disconnection of database servers from the network to capture volatile data. Evidence Collection process and Identification process are the two investigation processes that have been offered to retrieve fragile data from the database server. In the Identification process, the database server is disconnected from the network and forensic environment, and forensic techniques are provided to move the data already captured.

On the other hand, in the Evidence Collection process, volatile data are gathered from compromised database servers. Forensic research is necessary to recover and store carefully the volatile data to be used in later analyses. It allows forensic inspectors to gather non-volatile data in a "human-readable" form, which can be observed more easily compared to its stored binary version.

The fifth model, which is termed the detection investigation forensic model, was designed in [35]. This model addressed the ways an examiner can find evidence of data theft when there is no auditing. Their model reveals the way an Incident Responder/DBA might determine in cases where such a breach of an Oracle Database server occurs in a case in which no audit trail exists, but the assumption is that an attacker has obtained unauthorized select access to data.

The researchers in [42] suggested the SQL server forensic analysis method in 2008. The method they proposed could be used to gather and analyze the evidence from the MSSQL server database. Four phases were involved in the method: preparing the investigation, verifying the incident, collecting artefact, and analyzing the collected artefact. This was completely focused on the SQL server database.

Moreover, in [49], the authors designed another database server detection and investigation process model. The main objective was the detection of database servers and the collection of required data. The model comprised three phases: detecting the server, gathering the data, and examining the data. Though, this model is not able to work on volatile artefacts.

In [46], the detection inconsistencies database model was formed for the aim of identifying and naming the bytes and interpreting them for the MySQL database system. Using that knowledge, the users will be capable of detecting the discrepancies that appear within a database. Nevertheless, according to Khanuja and Adane [29], no knowledge has not been found for multiple log files and cache for more analyses. The model made use of the MySQL database server log artefacts.

In addition, in [55], the researchers designed a reconstruction model to reconstruct the basic SQL statements from redo logs restoring the already-deleted or updated values. Although, their proposed model was centered upon the DML statements, and the basic DDL statement was overlooked.

The authors in [65] proposed a practical forensic approach in a way to reconstruct the basic SQL DDL statements, aiming at improving the previous approach.

In another study [29], a framework was introduced that can be used for identification, collection, analysis, validation, and documentation of digital evidence in such a way to find out malicious tampering. The framework contained the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

following phases: Gathering and analyzing non-volatile data, Gathering, analyzing, reconstructing the volatile data, and making a comparison on the obtained results.

Regardless of the different database forensic domain knowledge projected for DBMS, several forensic tamper detection models and analysis algorithms of database systems have also been introduced by different scholars in the literature. For instance, [36] discovering methodology and scenario were proposed for the detection of covert database systems in a way to help investigators in the process of discovering and detecting covert database systems.

The researchers in [84] designed a model to efficiently collect digital evidence. It was able to gather evidence from a database business environment against authorized and unauthorized events. Their model made use of database features like triggers, replication, and log file backup.

In a scientific project [85], the authors designed a forensic tamper detection model capable of detecting a compromised database audit log by utilizing a strong one-way hash function. Nevertheless, it also suffered from a drawback as it was not able to analyze intruder activities and it failed to decide the time tampering occurs and which data were changed; it also was not efficient in identifying the adversary.

In a model was introduced mainly for the investigation of a compromised database management system. Two examination processes were involved in the model, namely identification and collection. The former prepares database forensic layers, methods, as well as the forensic environment; whereas the latter allows the user to collect doubted database management system data and transfer them into a secure place for further forensic examinations.

In [67], the scholars proposed a model for collecting, preserving, and analyzing the database metadata against database attacks. Their proposed model contained four investigation processes: collecting and preserving, analyzing the anti-forensic attacks, analyzing the database attack, and preserving the evidence report.

In another study [69], a novel model was introduced aiming for reconstructing the database events in a way to effectively discover intruder actions. Two investigation processes involved were collecting and reconstructing the evidence. In the former, evidence is gathered through replicating sources while in the latter the activities of user are rebuilt, and malicious activities are detected.

Additionally, several forensic algorithms, and tools have been proposed in the literature for the database forensic. For example, tampering on database audit log can be detected by using strong one way hash function [85]. Therefore, any compromised-on database audit log will detect. However, this algorithm cannot analyze intruder activities and decide when the tampering occurred, what data were altered, and ultimately, who is the adversary. Therefore, several forensic analysis algorithms have been developed for this purpose such as. Monochromatic, Red Green Blue (RGB), Red Green Blue Yellow (RGBY), Tiled-Bitmap and a3D algorithms. These forensic algorithms have different capabilities to analysis collected data in term of time and cost, for example Monochromatic algorithm can detect one corruption event, whereas RGB can detect two corruptions events, however RGBY may detect more corruption events but with false alarms. The limitations of these algorithms have not generalizable and inadequate characterization of the space of possible corruptions and the concomitant. Also lack of understanding of the comprehensiveness of extant tamper detection [58].

On the other hand, a few forensic tools have been proposed in the literature for database forensic field which are SQL Profiler (MS SQL Server) [86], ProfilerEventHandler (My SQL) Khanuja and Adane [29], and Log Miner (Oracle DB) [32]. SQL Profiler is a graphical tool that allows system administrators to monitor events in an instance of MS SQL Server. It has a capability to gather and save whole information about each operation/event to a file or SQL Server table to analyse later. The ProfilerEventHandler is a tool in MySQL implements the interface that is used to handle profiling and tracing the events [29]. The Log Miner tool has been developed by Wright [32] that allows a DBA or forensic analyst to reconstruct actions that took place on a database.

On the other hand, this paper involves the existing forensic works which focused on NoSQL database systems. For example, [28] proposed a forensic investigation framework for the document store NoSQL DBMS based on its unique features. It consists of five phases which are: preparation, acquisition and preservation, distributed evidence identification, examination and analysis, and reporting and presentation. However, the proposed framework not comprising the evaluation for the scheme of a database, or database forensic characteristics for example, gathering logs for operation assessment.

A forensic tool was proposed by [87] to investigate the internal structure and data file format of one of the most widely used NoSQL DBMSs, the MongoDB, and researched a method to recover deleted data. However, this tool does not support WiredTiger, the default storage engine in versions MongoDB 3.2 and higher.

Apart from the proposed existing works for the database forensic field, there are also a few review/survey papers proposed in the literature. For example [88] proposed a review paper for database forensic investigation processes that presented a broad literature review of the database forensic field that will help domain researchers in realizing database forensic from different views, as well as discussed the issues and drawbacks and suggested some solutions for the revealed issues. [89] conduced review on the database forensic field from 2009 to 2015. Only 282 articles have been discovered from 8 search engines. However, authors focused on normal review, they didn't mention the limitations, challenges, issues, direction, or any proposed solution for database forensic field. [80] conducted systematic literature review for database forensic field for period 2015 to 2017. Two search engines were used to collect data: science direct and IEEE Explore. The authors

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

came with proposed a forensic analysis model for the database forensic field which is consists of five stages: defining, identifying, preparing, comparing, recovering, distributing, acquiring, carving, collecting, restoring, audit log, determining event, examining, and presenting, documenting, reporting. Comparing with the existing review/survey papers, this review paper has covered wide areas of the database forensic field as shown in Table 2.

Table 2. Comparative analysis of current review paper and existing review papers for database forensic field

Coverage Area	Current Article	Existing Review Papers		
		[88]	[89]	[80]
NIST standard mobile forensic procedures	✓	✓	✓	✓
Proposed solutions	✓	✓	×	✓
NoSql Database systems	✓	×	×	×
RDBMS	✓	✓	✓	✓
DBMS Dimensions	✓	×	×	×
Standardization	✓	×	×	×
Forensics Readiness	✓	×	×	×

Clearly, the paper covered many aspects of the database forensic field comparing with existing review papers. It covered most of database forensic tools, algorithms, processes, for both RDBMS and NoSql database systems. The review presented in [88] focused on database forensic field from investigation process perspective only. Furthermore, the study reviewed 40 investigation process models of RDBMS, which do not cover the existing database forensic tools or algorithms. Also, the study did not cover forensic perspective of the NoSQL database systems. Similarly, the review presented in [89] conducted normal review, which failed to mention the limitations, challenges, issues, direction, or neither was any proposed solution for database forensic field provided. In a similar review studies, a review of relational DBMS was considered [80]. The study proposed a forensic analysis process model for RDBMS. However, the study did not cover other aspects of the database forensic field.

Based on the existing literature, the database forensic domainhas suffered from numerous issues as shown in Figure 4:

1. *Lack of common database forensic tool*: each database system has a specific forensic tool, for example, Oracle database forensic has Log Miner, and SQL queries and MSSQL server has specific SQL tools, etc. the common/generic database forensic tool is highly required.
2. *Redundant terminologiesand processes*: each database systemhave a specific investigation process and terminologies which produced numerous investigation terminologies and processes which make the database forensic field unstructured and unorganized amongst domain forensic practitioners.
3. *Different infrastructures and multidimensional nature of the database systems*: one of the major limitations facing database forensic researchers and theforensic communities differing of database system infrastructure and multidimensional nature of these systems. each database system has a different logical and physical architecture, as well as has three dimensions (internal dimension, logical dimension, and external dimension).
4. *Various Forensic Investigation Artifacts*: the variety of database system architecture produced various and different forensic artifacts with similar names and different meanings. Thus, produced confusion among database forensic investigators. For example, log files in Oracle database forensics, equivalent five log files in the MySQL database forensics (error log, general query log, binary log, slow query log, and the relay log), equivalent four log files in the Microsoft SQL Server (Windows event log, SQL Server agent log, SQL Server error log and the transaction log), equivalent two log files in PostgreSQL (transaction log, and the Server log), equivalent three logfiles in Oracle database forensic (redo logs, the archived redo logs and the alert logs), equivalent two log files in the DB2 (database recovery log, and the diagnostic information log), and equivalent two log files in the Sybase database (the transaction log and the message log).

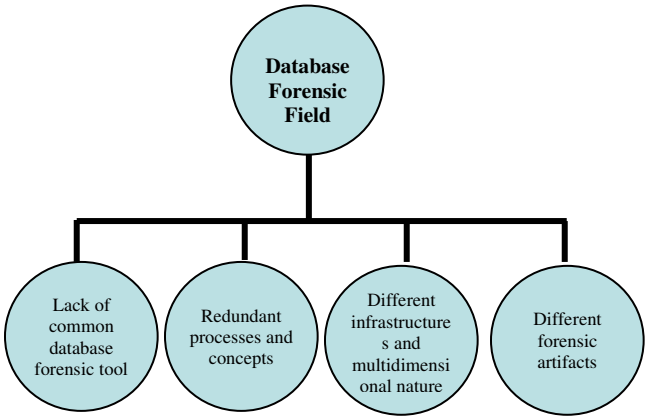

Figure 4. Major database forensics issues

IV. MOBILE FORENSICS

Mobile forensics involves the recovery of digital evidence from mobile devices through the use of scientific investigation techniques [90], [91]. Mobile forensics has become a significant subdomain since, on the one hand, services based on mobile phones are increasingly growing and more users are getting attracted to them. On the other hand, mobile commerce and mobile computing are gaining wide adoption. With such a relatively high adoption tendencies, coupled with the potential for misuse, this subdomain of presents a major forensic and security consideration. This section introduces a brief review of mobile forensics literature as shown in Table

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

3. It further discusses the limitation and drawbacks associated with this subdomain.

For example, the [92] tested wireless devices manufactured by BlackBerry from a forensic point of view. In another project [93], an innovative tool, called PDD, was introduced for memory imaging and forensic analyses of devices that run the Palm OSs for PDAs. The researchers in [94],[95] suggested several processes, tools, and guidelines for PDAs, GSM, and Cellular mobile phone. In [96], a novel method was introduced for the extraction of evidence from internal memory and SIM cards in the case of GPSs, mobile phones, and PDAs. The researchers in [97] suggested a SIMbrush tool capable of extracting a full file system for Linux, mobile phones, and Windows platforms. In another study [98], an on-phone forensic tool was proposed for the extraction of evidences from active files on mobile phones. From the research in [99], the authors introduced a tool with the capacity of extracting pieces of evidence from internal flash memory CDMA mobile phones for Korea CDMA mobile phones.

The researchers in [100] worked on flasher devices of mobile phones. In [101], a database-driven approach was suggested for the evaluation of mobile phone acquisition tools. In another scientific project [102], a guideline was suggested for cell phones and a full discussion was provided concerning all of the acquisition types. In Breeuwsma et al [103], a recovery approach was offered for extracting both videos and images from memories of mobile phones flash. In another research [104], a recovery method was introduced for the extraction of evidence (both file and videos) already removed from NAND flash memories. The authors in [105] proposed two approaches: an identity module programming for SIM cards and phone manager protocol filtering. In [106], a physical acquisition method was suggested for iPhone. The researchers in [107] provided a comprehensive discussion about the evaluation of mobile internal acquisition tools and logical acquisition. The authors in [108] introduced the hashing techniques applicable to mobile forensics. In [109], problems with Symbian forensics and all of the methods proposed in the literature for the acquisition purpose are discussed. In another project [110], from a forensics viewpoint, the Windows Mobile and Symbian ones were compared to each other. In [111], a certain process model was designed to analyze the Symbian smartphones from a forensic perspective (it included five phases). The researchers in [112] presented a discussion about all of the acquisition methods proposed for iPhone. In [113] an innovative method was introduced for Symbian devices on the basis of data reverse-engineering.

In a study conducted by [114], a model was designed for the extraction of messages, call recordings, contacts, documents, and scheduling together with all acquisition methods in a way to be applied effectively to Windows Mobile. In addition, the scholars in [115] made an effort to develop a model for the extraction of evidence from wireless connections in the case of Windows mobile.

In [116], an inclusive discussion was presented about the logical acquisition in the case of a Blackberry device. The authors in [117], designed a novel method and a device to acquire data from memory cards, including the memories of types of mini SD, SD, and MMC in the case of both Windows and Symbian mobile devices. The authors in [118], attempted to carry out the first studies into Android forensics and presented all of the methods adaptable for acquiring data from devices running with the Android system.

In [119], a discussion was presented regarding physical methods of data acquisition that can be used only in non-password protected devices utilizing the pseudo-physical acquisition for Windows Mobile. In another study [120], commonly-adopted methods for the extraction of evidence from GPS in mobile were discussed. In [121], tested the physical and logical techniques for acquiring data in case of the Sony Xperia 10i. The researchers in [122] attempted to develop an innovative framework for forensic acquisition and analysis applicable to the devices with Android system. In [123], a discussion was provided about three methods for extracting data such as photos, and messages from mobile phones. The authors in [124] presented all of the acquisition methods in literature and centered upon how to recover the data already removed from smartphone devices; then, they introduced innovative methods for analysing fragmented flash memories. In [141], a novel method as well as a set of tools were proposed to physically acquire evidence from volatile Android memories. The researchers in [146] attempted to suggest a way to analyse WhatsApp on Android-running smartphones from a forensic perspective. In [143], a logical data acquisition process was introduced in the case of Blackberry devices. The authors in [179] offered some techniques that can be effectively adopted to extract evidence from those Android smartphones that are encrypted. In [156], several support systems were introduced to efficiently preserve the evidence in Android phones. In another research [180], the authors attempted to compare the forensic acquisition methods proposed in the literature for Android devices. In [181], the researchers attempted to develop some techniques for the aim of interpreting the contents of raw NAND flash memory images. In [160], a full discussion was presented concerning the analysis of WhatsApp chat upon the smartphones running with the Android system in a way to recollect the already-removed messages. The authors in [163] introduced an adversary model for the facilitation of forensic investigation on mobile devices working with different systems such as iOS, Android, and Windows. The model was designed in such a way to be readily adaptable to the state-of-the-art technologies in mobile phones. In [182], the scholar offered a combination of suspicious pattern detection and criminal profiling methodology in case of two criminal actions with moderate-to-heavy involvement of mobile devices, low-level drug dealing, and cyberbullying. In [183], a novel approach was suggested validating the mobile forensics tools and the data that are stored upon the devices.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

From this survey, it can be said that most of the current research have not focused on fundamental and essential guidelines for establishing a baseline for the mobile forensic field, but focused instead on specific procedures and principles of technical issues in solving specific problems. Thus, the mobile forensic field is suffering from several issues:

1) Lack of unified mobile forensic model: due to the variety of the OS and infrastructure of the mobile devices, numerous MF models have been Offered in the literature. Each MF has a unique investigation/examination model which have different investigation processes and tasks. Thus, the lack of a unified and harmonized MF model.
2) Lack of unified investigation processes and terminologies: the variety of the OS and infrastructure of the mobile devices have produced different investigation processes and terminologies. These different and varying investigation processes and terminologies make the MF field ambiguous and complex amongst MF practitioners. Thus, the MF field lacks unified investigation processes and terminologies.
3) Mobile devices architectures: the different infrastructures of mobile devices consider the main dilemma for the MF developers and researchers. Each mobile device has a different logical and physicalinfrastructure.
4) Various Forensic Investigation Artifacts: the variety of mobile device architecture produced various and different MF artifacts with similar names and different meanings. Thus, produced confusion among MF investigators.

Table 3. Mobile Forensic Models

Year	Mobile Forensics Models	Mobile Type & OS	NIST standard forensic procedures			Type of the Model		Digital Forensics Readiness			Decreases Heterogeneity and Ambiguity	
			Preservation	Acquisition	Analysis	Reporting	Technical	Conceptual	Adopt pre-incident preparation	Provides Mean of Assessing for forensics	Offer Interoperability Environment	Offer Unified Platform
2002	[92]	BlackBerry	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2002	[93]	PDAs	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2003	[94]	GSM	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
2004	[125]	PDA	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
2004	[95]	Cellular mobile phone	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2005	[96]	Mobile phones, PDAs, and GPSs).	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2006	[97]	Mobile phone Linux and Windows platforms	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
2007	[98]	Symbian	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
2007	[99]	Korea CDMA mobile phones	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
2007	[100]	Mobile phone	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
2007	[101]	Mobile phone	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
2007	[102]	Mobile phone	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
2007	[103]	Mobile phone	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2008	[104]	Mobile phone	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2008	[105]	Mobile phone	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
2008	[106]	iPhone	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2008	[107]	Symbian	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
2009	[108]	Smartphones	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
2009	[109]	Symbian	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
2009	[110]	Symbian and Windows Mobile devices.	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
2009	[111]	Symbian	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2009	[113]	Symbian	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2009	[114]	Windows Mobile	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
2009	[115]	Windows Mobile	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2010	[116]	Windows Mobile.	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗

2010	[118]	Android phones.	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
2010	[119]	Windows Mobile	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2010	[126]	iPhone.	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
2010	[127]	Symbian.	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
2010	[128]	Windows Mobile.	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2011	[129]	iPhone.	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2011	[120]	Symbian.	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
2011	[130]	iPhone.	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2011	[131]	Windows Mobile.	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2011	[122]	Android.	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2011	[132]	Android.	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
2011	[133]	Android.	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
2011	[134]	Android	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
2011	[135]	Smartphones	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
2011	[136]	Smartphones	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
2012	[123]	Android & windows mobile	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2012	[137]	Symbian	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
2012	[138]	General	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
2012	[139]	BlackBerry Torch 9800, iPhone 4, and the Android-based Samsung Galaxy S	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2012	[140]	Smartphones	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2012	[124]	Android and iOS devices	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2012	[141]	Android	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2012	[142]	Android	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2012	[143]	Blackberry	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2012	[144]	Smartphones	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗
2013	[145]	Android	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2013	[146]	Android	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
2013	[147]	iPhone	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2013	[148]	Android	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2013	[149]	Windows Mobile	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2013	[150]	iPhone and iPad devices	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2013	[151]	Android	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
2013	[152]	Android	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2013	[153]	Android	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗
2013	[154]	iPhone and iPad devices	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2013	[155]	Smartphones	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
2013	[156]	Android	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
2013	[157]	Android	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
2013	[158]	iPhone and Android	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2013	[159]	Smartphones	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2014	[160]	Android	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2014	[161]	Android	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2014	[162]	Android	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
2015	[163]	Android,	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2015	[164]	Android	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
2016	[165]	General	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗
2016	[166]	Android	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
2016	[167]	Android	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2017	[168]	General	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓
2018	[169]	iOS system	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗
2019	[170]	Android	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2019	[171]	Android	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2019	[172]	Android	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
2021	[173]	Smartphone	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
2020	[174]	General	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗
2020	[175]	General	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗
2021	[91]	General	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2021	[176]	General	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
2021	[176]	General	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
2021	[177]	Android	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗
2021	[178]	Android	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

A further comparison of the current review with other existing reviews in given in Table 4.

Following the diverse coverage areas of mobile forensics, existing reviews attempts to provide insight from few coverage-scope. The current review provides comprehension that include forensic readiness, and standardization. These notions have been largely ignored by existing review, yet they represent a growing body of research work on mobile forensics. The potential of a unified forensic framework is also lacking in these review works.

Table 4. Comparative analysis of current review paper and existing review papers for mobile forensic field

Coverage Area	Current Article	Exciting Articles			
		[91]	[184]	[185]	[186]
Mobile OSs	✓	✓	×	×	✓
NIST standard mobile forensic procedures	✓	✓	✓	×	✓
Forensics Readiness	✓	×	×	×	×
Standardization	✓	×	×	×	×
Mobile Forensic Challenges & Issues	✓	✓	✓	×	✓
Mobile malware detection	✓	×	×	✓	×
Proposed Solution	✓	×	×	×	×

V. NETWORK FORENSICS

As defined in [187], network forensics either on-the-fly or post-mortem can be defined as the branch of digital forensics that addresses network-related investigation. This includes the identification, extraction, interpretation, event-reconstruction, analysis, and documentation of network-related events in a way that ensures the evidential value and integrity of the collected data. Such evidential data are then used to corroborate, and or correlate informed hypotheses and assertions about a networking event. Therefore, network forensics, primarily, aims to explore network-based attacks through the identification and extraction of critical network-based indicators, which can potentially be used to complement network security posture, develop network readiness processes as well as enhance the probative evidential weight of potential network artefacts [188]–[190]. The growing trend of network-related threats and the increasing sophistication of network-based attacks have further necessitated the delineation of this subdomain. An offshoot of this subdomain can be further classified as cyber forensics, as most network-based attacks are depicted as cyberattacks. Today, numerous cyber-attacks or cybercrimes are occurring maliciously across the world. Network forensics has been shown to have the capacity to providing investigative capability, capable of deterring and preventing (where possible) some complex cyber incidents. This field of study consists of numerous models applicable to process investigations. For instance, in [191], the authors introduced a distributed network logging model capable of adding cyber forensics over the internet. In addition, in [192], a network forensics model was developed, which was dependent upon distributed techniques. Such techniques are used to provide a single platform to gather forensic evidence automatically, effectively storing the collected data, and supporting the easy integration of well-known attribution methods. In another study [193], a dynamic forensic network model was designed based on an immune agent aiming for capturing and storing digital evidence that has leaked through the network. Their model comprises the distributed data agents and the forensic center.

In [194], the researchers introduced a generic network forensic process model through the extraction of the most important characteristics from currently-used digital forensic process models and incorporation of those characteristics in their model. In [195], a common model for network forensics in Infrastructure-as-a-Service (IaaS) has been developed. An architecture for "Forensics-as-a-Service" in a cloud management infrastructure has been defined. This architecture offers an authorized environment subjects that can use to remotely control the forensics process at the cloud provider. Both data acquisition and data analysis can be handled directly at the cloud provider. A reference model of a distributed cooperative network forensics system has been proposed by [196]. It can speed up the investigation and enhance the capability of the emergency response. The aim of the proposed model is putting the misbehavior activities/traffics on the root of adaptive location filter guidelines of discarding in advance or in real-time, evaluating the total supportive database to determine the possible misbehavior, restating the misbehavior for the investigation of forensics. The network forensics model which constructed on the scattered methods thus offering a unified model for automatic forensic evidence gathering and effective data storing, a supportive informal combination of recognized attribution approaches, active collaboration, and an attack attribution display production method to demonstrate hacking measures. Furthermore, a theoretic and official information model for forensic computerization on online community networks has been proposed by [101]. It contains an event-based knowledge model, which offers theoretic ideas that can support the building and explanation of the actions associated with the event under examination. The proposed model is applied through an ontology to offer a semantically rich and proper image to the concepts.

A novel network forensic framework, named "Particle Deep Framework", created on optimization and deep learning was provided by [102]. The optimization method based on Particle Swarm Optimization (PSO) to choose the hyperparameters of the Deep Neural Network (DNN) was used.

Through this review and analysis, numerous network forensic models, frameworks, and processes have been offered to give solutions for network crimes, however, they did not consider the whole stages of examination. Most of them depend on a general record scheme, where analytical and interaction data are distributed between various units, such as the police and insurance corporations. The advantage of such a scheme would be that during an examination, all related data could be easily accessible to forensic specialists, while its reliability would be secured via digital signatures.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

Nevertheless, most of the network forensic frameworks and models concentrated on data collection rather than studying the whole forensic investigation process as shown in Table 5. These frameworks and models produced some drawbacks such as the breach of confidentiality, as a user's information is delivered between the participants and the additional difficulty that these models and frameworks need. Moreover, the existing frameworks and models concentrated on the protection and gathering stages of the investigation. Additionally, the analyzing data, including the variety of data sources, data granularity, data integrity, data as legal evidence, and privacy issues are the major drawbacks of network forensics. These drawbacks can be put in the three general groups: technical, legal, and resource.

Through this survery, it is clear that the network forensic field is suffering of lacking comprehensive model/framework to combine whole redundant and overlap network forensic concepts, processes, tasks, and activities. Table 6 shows the comparison between the current review paper and existing network forensic review papers.

Similar to the reviews on mobile forensics, existing reviews on network forensics have largely ignored the growing research on forensics readiness and attempts towards standardization. The current review therefore provides a holistic review of existing literature in the network forensics subdomain.

Table 5. Network Forensic Models

Year	Mobile Forensics Models	NIST standard forensic procedures				Type of the Model		Digital Forensics Readiness		Decreases Heterogeneity and Ambiguity	
		Preservation	Acquisition	Analysis	Reporting	Technical	Conceptual	Adopt pre-incident preparation Approach	Provides Mean of Assessing for forensics readiness	Offer Interoperability Environment	Offer Unified Platform
2004	[197]	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
2005	[198]	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
2007	[199]	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
2007	[200]	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗
2010	[201]	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗
2010	[202]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2010	[194]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2012	[203]	✓	✓	✗	✗	✓	✓	✓	✓	✗	✗
2012	[204]	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
2012	[205]	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗
2012	[206]	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2013	[207]	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗
2013	[208]	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2013	[209]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2013	[210]	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗
2013	[211]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2014	[212]	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
2016	[213]	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
2018	[214]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2019	[215]	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
2019	[216]	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗
2019	[217]	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗
2019	[218]	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗
2020	[219]	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
2020	[220]	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2021	[221]	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

Table 6. Comparative analysis of current review paper and existing review papers for network forensic field

Coverage Area	Current Article	Existing Review Papers		
		[187]	[194]	[222]
NIST Standard Network procedures	✓	✗	✓	✗
Forensics Readiness	✓	✗	✗	✗
Standarization	✓	✗	✗	✗
Network Forensic Challenges & Issues	✓	✓	✗	✓

VI. IoT FORENSICS

Internet of Things (IoT) Forensics is a process of identifying, acquiring, organizing, investigating, and presenting an attempt to explain an attack with all required details [223]. The digital forensics techniques have not completely adopted IoT forensics since the currently used digital forensics tools and processes cannot satisfy the distributed nature and heterogeneity of the IoT infrastructures. The scholars who work in the digital forensics field of study have proposed several conceptual process models capable of guiding forensic investigations, including IoT forensics. Different attempts made for the development of this branch of study are still at their initial steps, and the studies carried out in this context show an emphasis on developing theoretical process models based on hypothetical case studies. IoT forensics is generally conducted at three forensics levels, namely Network level forensics, Cloud level forensics, and Device-level forensics. To the best of our knowledge, Internet of Things forensics has not been completely used so far in digital forensics techniques, and this is because the currently-used digital forensics tools and processes cannot satisfy the distributed nature and heterogeneity of the IoT infrastructures [6], [224], [225]. Therefore, collection, examination, and analysis of potential evidence from IoT environments, which can be employed as evidence acceptable to a court of law, make a big challenge to digital forensics investigators and Law Enforcement Agencies (LEAs) [226]. Several models have been designed aiming for guiding the forensic investigations, which involves also IoT as shown in Table 7. Such efforts are still in their infancy, and they are significantly focused upon developing theoretical process models based on hypothetical case studies.

Table 7. IoT Forensic Models

Year	IoT Forensic Investigation Models	NIST standard forensic procedures				Type of the Model		Digital Forensics Readiness		Decreases Heterogeneity and Ambiguity	
		Preservation	Acquisition	Analysis	Reporting	Technical	Conceptual	Adopt pre-incident preparation Approach	Provides Mean of Assessing for forensics	Offer Interoperability Environment	Offer Unified Platform
2015	[227]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2016	[224]	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗
2017	[228]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2017	[229]	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
2017	[230]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2018	[231]	✓	✓	✗	✗	✗	✓	✓	✓	✗	✗
2018	[232]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2018	[233]	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗
2018	[234]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2018	[235]	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗
2018	[236]	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
2018	[237]	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗
2019	[223]	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗
2019	[238]	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗
2019	[239]	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
2019	[240]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2020	[241]	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
2020	[242]	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2020	[243]	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗
2020	[244]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
2020	[245]	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗
2020	[246]	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

2020	[247]	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗
2020	[248]	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
2021	[249]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2021	[250]	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗
2021	[251]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2021	[252]	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗
2021	[253]	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
2021	[254]	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗
2021	[255]	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗

For instance, the triage model of Next Best Thing (NBT) was developed responding to challenges that may arise during the forensic identification stage. It was aimed to help researchers to determine the potential evidence sources [256]. For NBT, it is recognized that devices together with any original evidence stored on them might get inaccessible or compromised because of different incidences such as destruction, theft, or tampering. As a result, investigators should be capable of recognizing the other elements of the IoT ecosystem, which pertain to the original device in question. This is since such elements could consist of items with evidentiary values.

In the same way, combining the techniques and resources from all of the digital forensic areas that are involved in an IoT investigation can shape a conceptual construct of IoT forensics [257]. Such a construct can be employed as a basis for the Forensic Aware IoT (FAIoT) model. The model proposed in the study makes use of a centralized and secure evidence logging, provenance, and preservation service to effectively address the problem of deficiency of standardization in the IoT ecosystem. On the other hand, the study did not discuss the practical context of the proposed model. The reason is that this issue has not been tested practically. Moreover, it encompasses only partial of artefact acquisition. In [248], the authors introduced a model for performing the forensic investigation and tracing the source with the use of network forensics to detect the harmful packets within the infected device. In [228], an innovative IoT forensic model termed PRoFIT was designed, which made sure of privacy (ISO/IEC 29100:2011) standard in the course of forensic investigation. The researchers in [229] introduced an IoT real-time model comprising two investigation phases: the pre-investigation and the real-time investigation phases. This model works in a way to make sure of the collection of required data and evidence and preservation of the collected data and evidence during the investigation course. In another research [6], a novel readiness IoT forensics model termed Digital Forensic Readiness (DFR) was designed. In this model, an architecture was configured with the forensic capacity of the incorporation of DFR to the IoT domain; the main objective was to have appropriate planning and to get well prepared for security cases that may potentially take place within an IoT environment. The model comprises three different phases: proactive, IoT communication mechanism, and reactive process phases. The authors in [231] introduced a digital forensic investigation framework for IoT termed DFSF-IoT. Their framework is mainly centered upon the establishment of digital forensic readiness and the increase of the permissibility of the evidence that is taken out of a device through process concurrency. The framework contains three processes: proactive, IoT forensics, and reactive processes.

The authors in [230] attempted to develop an application-specific digital forensics investigative model in Internet of Things. Their model contained three independent mechanisms: Application-specific forensics, digital forensics, and forensics process. Based on the type of investigated application, information flows among these components. The notion of functional requirements and processes model were introduced by the researchers [115] with the use of DFR process as a security component within an IoT-based environment. Their model introduces some aspects that are applicable as essential building blocks in the DFR technologies implementation process, which can guarantee the security within the IoT-based environments.

In [244] , a novel framework was designed and applied to the identification of IoT devices using their Genes, which results in the formation of the DNA structure of devices. In another research Scheidt and Adda [245], an innovative approach was proposed to the processes of forensic investigation and sharing data in a forensic environment. They also introduced models for the computation of the confidence values of an investigation in a way to make sure of an extremely valuable process for both retrieving and presenting the collected evidence.

In [253], the blockchain-assisted shared audit framework (BSAF) was designed, which was applicable to the analysis of digital forensic data in an IoT platform. BSAF was found capable of detecting the source and/or cause of data scavenging attacks within virtualized resources (VR). To gain access to log and control management, this framework made use of the blockchain technology. A forensic model was proposed in [246] , and also it was discussed what is the best way to set up an IoT testbed/lab for training inexperienced forensic investigators and aid them in examining the devices of interest and potential evidential sources. The authors validated the performance quality of their proposed model by applying it to some case studies.

The researchers in [247] were concentrated upon examining how to extract and analyze forensic artifacts from the Google Home and Google Assistant apps installed on an Android smartphone and how to apply them to controlling a Google Nest device (Google Home Mini smart speaker). They attempted to contribute to the body of knowledge in this field by exploring and analyzing the client-centric and cloud-native forensic artifacts. In [258], IoT forensics was

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

comprehensively reviewed. The authors, first, systematically discussed the issues related to IoT security. After that, they reviewed a number of significant issues in this field, including the IoT forensics (by emphasizing the necessity of applying Artificial Intelligence (AI) to IoT forensics), state-of-the-art research, identified opportunities, and the most important factors to succeed in IoT forensics process. They also discussed the current challenges in IoT forensics and attempted to suggest effective solutions to them. Then, the paper ended with discussing some open-research directions that are worth considering in this field. In [259], the authors suggested an IoT forensics taxonomy and discussed the challenges and limitations associated with IoT forensics. After that, a comparison was made between conventionally-used digital forensics and IoT forensics. Then, two models introduced for IoT forensics investigation were reviewed. Remember that is spite of the many opportunities provided by IoT, it is also associated with some grave concerns in terms of privacy and protection. In addition, investigators face important challenges when discovering crime scenes in IoT-based applications. On the basis of the two models discussed, the authors concluded that the models proposed for IoT forensics investigation purposes work differently and they suffer from different problems and deficiencies. As a result, there is not any specific standardized method or model applicable to IoT forensics investigations. The researchers in [249] attempted to present a concept methodology to carry out IoT forensics investigations using a conventionally-used model as the reference. It was mainly aimed at collecting the common features of all IoT devices and systems into a concept proposal covering the entire investigation process in such a way that it could be relied upon as a general guideline and also be applied to developing effective processes for addressing specific IoT contexts. The key goal of the authors in [250] was examining the significance of digital forensics readiness for companies, particularly from the perspective of IoT forensics. They attempted to identify and discuss the most important factors that affect the IoT forensics investigations. To end with, a readiness framework was proposed and validated in their study. In [251], a comprehensive preventive cyber forensic process model was derived with honeypots for the digital IoT investigation process. The model was designed in a way to help in a court of law to define the extent to which the investigative processes were reliable

Through this survey, it is clear that the Internet of Things Forensics suffers numerous issues as shown in Figure 5:

1. *The difficulty of supporting the newer IoT devices*: the current digital forensic tools and techniques do not support the newer IoT devices which created challenges for forensic practitioners to acquire data from these devices.
2. *Lack of strict security procedures*: due to the absence of high-security procedures and policies, this technology has been revealed to several weaknesses, which may cause cyber-incidents through the devices.
3. *Difficulties in applying the investigation process*: IoT forensic has six main investigation processes. The challenge involves how to utilize these investigation processes in tandem with IoT actions. The IoT devices generate an enormous amount of data containing possible evidence where it will affect the investigation process. Therefore, it is hard to detect which device had implicated in the crime and it will take more time to discover which devices introduce the crimes.
4. *Variety of Devices, OS, and Infrastructures*: the diversity, different OS, and the different infrastructures of the IoT devices make the IoT more complicated and complex. This condition may lead to various corruption or exploitation by the attackers. Thus, the various devices, OS, and communication channels may influence the investigation process.
5. *Lack of log standardization*: the investigation resources such as network logs, process logs, and application logs from various resources may assist the investigators to find an obvious knowledge of the complete action in the device. Nonetheless, there is the absence of a standard for logs resources through the various systems.
6. *Volatility of evidence*: The problems of evidence volatility in the IoT situation is much more difficult compared to traditional computing platforms, given that the sensor devices are low-memory devices.

Figure 5. IoT Forensics Issues

Existing review literature on IoT forensics have largely ignored some of the content presented in this manuscript. For example, a comparative analysis is given in Table 8.

Form the analysis presented in Table 8, existing review literature did not consider the implication of forensic

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

readiness and process standardization. The exclusion of these two coverage areas of IoT forensics presents a major oversight and limitation in the extant review literature. Therefore, the current review presents a holistic review. Furthermore, the current study proposed a harmonized model.

Table 8. Comparative analysis of current review paper and existing review papers for IoT forensic field

Coverage Area	Current Article	Existing Review Papers								
		[261]	[258]	[262]	[263]	[264]	[265]	[266]	[267]	[268]
NIST Standard Network procedures	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗
Forensics Readiness	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
Standarization	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
IoT Forensic Challenges & Issues	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

VIII. DISCUSSION

Through this survey, it is obvious that the DF field is a heterogeneous, complex, and unstructured domain, however wealthy domain for research. The study revealed and highlighted the different challenges and issues of the subdomains of mobile device forensics, network forensics, database forensics, and IoT forensics as shown in Figure 6. Thus, this section suggests a potential solution to address the identified research gaps as shown in Figure 6. These include:

- ✓ Subdomain-based metamodeling language: This can include attempts that aim to develop a formal language for the digital forensic domains using metamodeling approach. It would, however, require an initial metamodeling of the various subdomains that constitutes the digital forensic domain.
- ✓ Domain-based ontology: like the metamodeling approach, the use of ontology and semantics have been explored as an approach to develop a standardized baseline for domain. furthermore, the use of ontology for domain modeling towards domain language have also gained prominent concepts [269]–[271]. This approach can be used to reveal the degree of interdependencies among the various subdomains.
- ✓ Integrated framework for subdomains: studies have explored the potential of integrating diverse subdomain frameworks into a unified integrated framework. This logic can be adapted for the digital forensic domain. Investigation frameworks that can provide a reliable guide for developing a standard forensic process for the forensic domain remains a viable approach towards addressing some of the challenges identified in Figure 6.
- ✓ Harmonized integration process: Approaches that attempt to merge or harmonize processes from different subdomains presents a potential to address the growing diversity of process models among the various subdomains. This can be further leveraged to develop a mechanism for context-independent data collection process. However, this approach can further integrate semantic logic. In essence, the process of developing a harmonized approach can rely on the semantics associated with respective subdomain, to prevent redundancies.
- ✓ Structured representation of subdomain data: this is a major challenge within the digital forensic subdomain. Approaches that attempt to formalize data representation, and structured query of potential digital artefacts evidence representation (in a context independent manner) is a potential solution to data heterogeneity, and the lack of a unified data format. Furthermore, the development of a structure representation is a required step towards forensic automation. Forensic automation has been considered as a futuristic approach for digital forensics, which has the potential to reduce the dependencies on human errors. Consequently, reduce investigation biases, enhance evidence reliability as well as reduce investigation time. Automation in this regard refers to the act of using machines to carry out some forensic processes with minimal or no human oversight. For instance, studies in Singh et al [272] alluded to this assertion, as a requirement towards ransomware investigation.

As a step towards developing a subdomain metamodel, this study further proposed a metamodeling approach as a complementary process towards a generic digital forensic domain modelling.

A. Develop Metamodel for DF Subdomains (Semantic Metamodeling Language)

Whilst several studies have attempted to develop a unified; one-stop-reference for these proliferating subdomains within digital forensics, there seems to exist a lack of comprehensive reference sources that consider, specifically, the respective state-of-the-art in digital forensics subdomains. Such a reference model provides a baseline for exploring the distinction and similarities among the various subdomains. Knowledge of such a semantic and syntactic relationship is essential in any knowledge system [16], [116], [117]. Due to the heterogeneity and complexity of the DF subdomains, this study further suggests developing a metamodel to organize, structure, unify, share, manage, reuse, and facilitate the investigation task among domain forensic practitioners. The suggested metamodel is

hereinafter referred to as DF Metamodel (DFM). It integrates the common forensic processes, concepts, activities, procedures, tasks, attributes, and operations of the DF subdomains. The methodology used to develop DFM as adapted from [118] is further elucidated:

1) Detect and nominate DF subdomains models: In this stage, the construction and validation models were detected and nominated. Numerous DF models were reviewed and investigated in the existing literature review. The model chosen for this research will be based on coverage features that were recognized in the earlier study [118]. Wide coverage of DF subdomains that are broadly applicable is required to fulfill the aim of developing DFM. Using a coverage metric can quickly indicate sourced model applicability. The model is said to have a high coverage value if the model can cover most DF subdomains processes highlighted in the literature (i.e., a general model). The model has a reduced amount of coverage value if the model only describes partial DF subdomains.
2) Extract DF subdomains investigation processes: in this step, the DF subdomains investigation processes will be extracted from the selected DF models. During the extraction, certain criteria will be adhered to, to identify a relevant and proper investigation process. The criteria that will be used to identify the DF processes were adapted from [119]. These criteria's will be utilized to avoid any missing or random process selections:
   - ✓ Titles, abstracts, related works, and conclusions were excluded: the investigation process was either extracted from the diagram or the main textual model.
   - ✓ The investigation process must have a definition, activity, or task; to recognize the purpose and meaning of the process.
   - ✓ Irrelevant investigation processes not related to conducting DF subdomains will be excluded.
   - ✓ Include explicit and implicit investigation processes from models.
3) Merging and Grouping of the Extracted DF Subdomains Investigation Processes: The extracted DF subdomains processes will be merged and grouped based on similarities in semantic meaning or functional meaning. All investigation processes having similar semantic meaning or functional meaning will be organized, merged, and grouped into separate groups.
4) Propose common DF subdomains investigation processes: This step aims to propose a common investigation process for every investigation group highlighted in Step 3. The investigation process which has a higher frequency would be proposed as a common investigation process.
5) Develop the DFM: the proposed common DF subdomains investigation processes will be used to develop the DFM. The relationships amongst these processes will be then identified. The initial results of the DFM will be developed in this step.
6) Validate and demonstrate the DFM: this step is used to validate the completeness, logicalness, and usefulness of the proposed DFM through two validation techniques namely: Comparison against other models, and Face validity. A comparison against other models is used to verify the completeness of the first version of the DFM against existing domain models. The output of this validation is the second version of the DFM. A Face validity technique is often used to validate the completeness and logicalness of the second version of the DFM. Consequently, a third version is generated. This process typically involves a confirmatory analysis process where knowledge experts in the discipline are identified, and then required to verify the suitability, appropriateness, completeness, logical sequence of event, as well as the overall contextual applicability of a given model.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

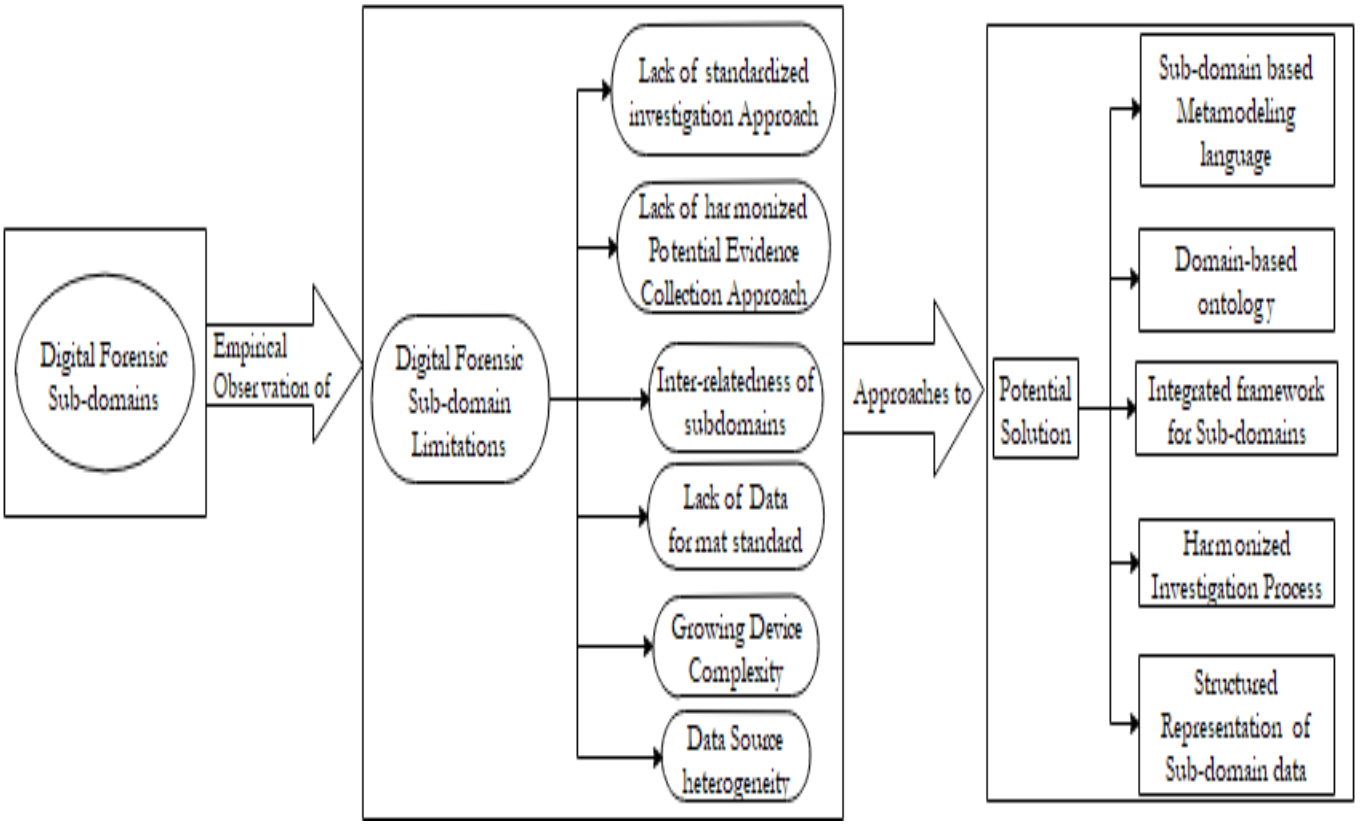

Figure 6. **Limitations and solutions for DF subdomains**

B. Initial Version of the DF Metamodel

The initial version of the DFM, as illustrated in Figure 7, consists of three levels: M2-Level (Metamodel), M1-Level (User Models), and M0-Level (User Data Models). The M2-Level contains meta-classes (meta-operations, and meta-attributes) which govern the behavior of the M1-Level. The M1-Level consists of Meta-Objects (metadata) which govern the behavior of the M0-Level. The M0-Level consists of the real data which represents the real scenarios of the DF subdomains. For example, the database forensic models in the M1-Level are instances of DFM, and the data models in the M0-Level are instances of M1-Level models. Thus, the DFM will allow domain forensic practitioners to instantiate/derive solution models for problems under investigation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

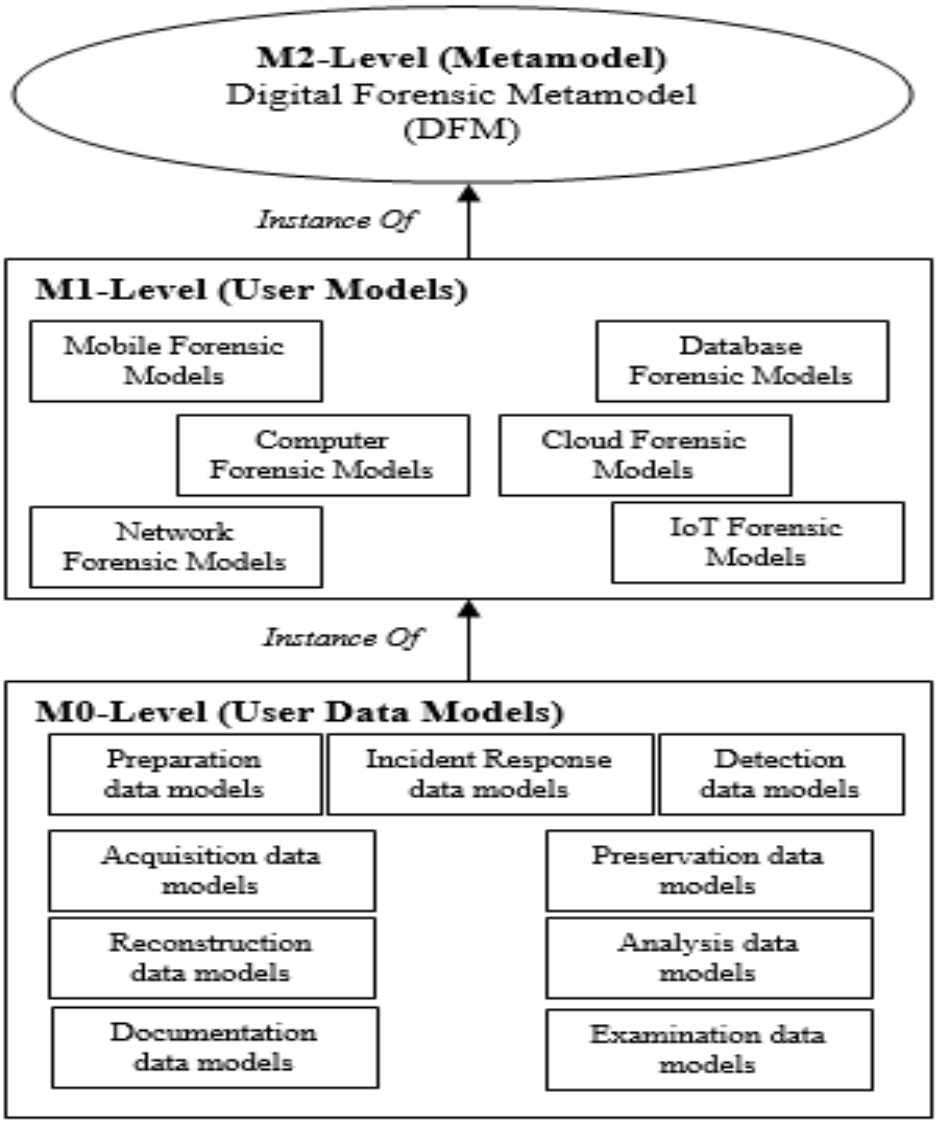

Figure 7. Initial version of DFM

To demonstrate the capability of the DFM, a scenario of a compromised database server was stated by [38]: "*A DBA believes that one of his development servers has been compromised. No auditing was enabled. Is there any evidence to support a compromise that occurred? The requirement is to develop a specific verification model to check availability of any evidence to support a compromised happened in several development servers when auditing feature was absent*".

The main activity of this scenario is checking the availability of evidence which includes several activities (e.g.*: Isolated Database Server* (); *Search Evidence* (); and *Identify Investigation Source* (). Therefore, M1-Verification Model is required to verify the availability of evidence against a compromised development server when the auditing feature was absent.

The M1-Verification Model illustrated in Figure 8 consists of many activities instantiated from DFM. These activities are derived from different sharing activities from different DFM processes and concepts and have enough information to guide domain forensic practitioners to verify the availability of evidence against a compromised development server. The guidelines that have been offered with this derived model assist domain practitioners to instantiate several real M0-Verification Data Models easily. For example, instantiate *M0-Identify Investigation Source Data Model, M0-Isolate Database Server Data Model, M0-Seize Investigation Source Data Model, M0-Incident Responding Data Model, M0-Acquire Data Model, and M0-Check Available Evidence Data Model* from M1-Verification Model.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3124262, IEEE Access

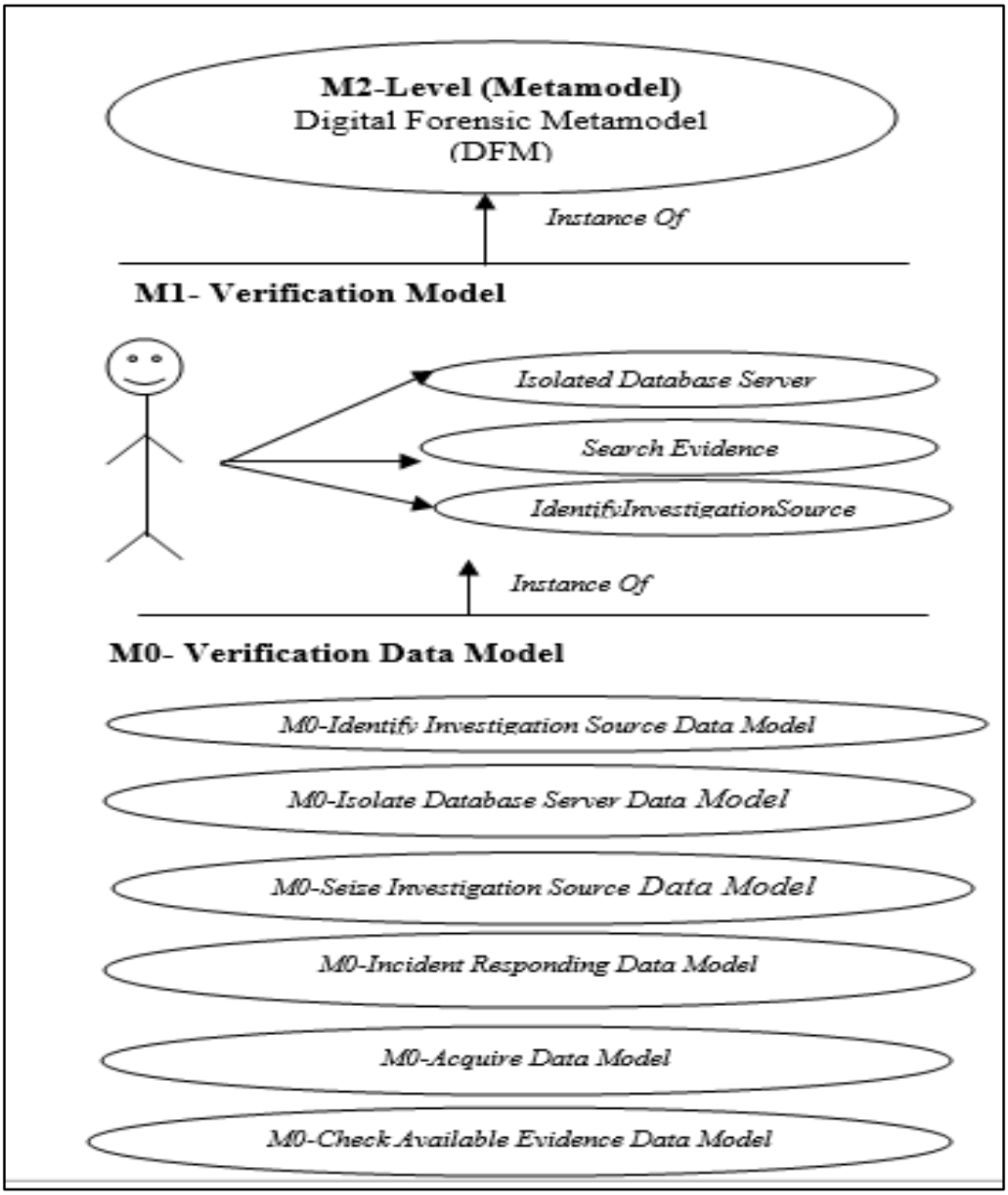

Figure 8. Instantiate Solutions models from DMF

VIII. CONCLUSION

This paper presented the results of a systematic literature review that examines approaches for investigating four digital forensic subdomains, namely: database forensics, mobile forensics, network forensics, and IoT forensics. One of our observations is the lack of standardization across the four subdomains. For example, we identified several different investigative models and processes proposed by the research community for these subdomains, and many of these models and processes were designed to address a specific scenario or problem within that subdomain. As a result, very few, if any models from one subdomain could be translated to an investigation involving a different subdomain or across subdomain(s). Hopefully, the findings from this paper will benefit the digital forensics community. The future work of this study is to develop and validate the DFM to solve the heterogeneity and complexity of the DF subdomains.

References

[1] W. Jansen and R. Ayers, "Guidelines on cell phone forensics," *NIST Spec. Publ.*, vol. 800, no. 101, pp. 101–800, 2007.

[2] C. P. Grobler, C. P. Louwrens, and S. H. von Solms, "A framework to guide the implementation of proactive digital forensics in organisations," in *2010 International conference on availability, reliability and security*, 2010, pp. 677–682.

[3] V. R. Kebande, N. M. Karie, R. A. Ikuesan, and H. S. Venter, "Ontology-driven perspective of CFRaaS," *Wiley Interdiscip. Rev. Forensic Sci.*, p. e1372.

[4] V. R. Kebande and H. S. Venter, "A comparative analysis of digital forensic readiness models using CFRaaS as a baseline," *Wiley Interdiscip. Rev. Forensic Sci.*, vol. 1, no. 6, p. e1350, 2019.

[5] A. Valjarevic, "Harmonised Digital Forensic Investigation Process Model," in *Information Security for South Africa*, 2012, pp. 1–10.

[6] V. R. Kebande, N. M. Karie, and H. S. Venter, "Adding digital forensic readiness as a security component to the IoT domain," 2018.

[7] H. Munkhondya, A. Ikuesan, and H. Venter, "Digital Forensic Readiness Approach for Potential Evidence Preservation in Software-Defined Networks," in *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019*, 2019, vol. 268.

[8] I. R. Adeyemi, S. A. Razak, M. Salleh, and H. S. Venter, "Leveraging human thinking style for user attribution in digital forensic process," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 7, no. 1, pp. 198–206, 2017, doi: 10.18517/ijaseit.7.1.1383.

[9] A. Singh, A. R. Ikuesan, and H. S. Venter, "Digital Forensic Readiness Framework for Ransomware Investigation," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2019, vol. 259, pp. 91–105, doi: 10.1007/978-3-030-05487-8_5.

[10] S. Omeleze and H. S. Venter, "Testing the harmonised digital forensic investigation process model-using an Android mobile phone," Aug. 2013, doi: 10.1109/issa.2013.6641063.

[11] S. O. Baror, R. A. Ikuesan, and H. S. Venter, "A defined digital forensic criteria for cybercrime reporting," *Proc. 15th Int. Conf. Cyber Warf. Secur. ICCWS 2020*, no. ii, pp. 617–626, 2020, doi: 10.34190/ICCWS.20.056.

[12] A. R. Ikuesan and H. S. Venter, "Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet?," *Digit. Investig.*, vol. 30, pp. 73–89, 2019, doi: 10.1016/j.diin.2019.07.003.

[13] D. Ernsberger, A. R. Ikuesan, H. S. Venter, and A. Zugenmaier, "A Web-Based Mouse Dynamics Visualization Tool for User Attribution in Digital Forensic Readiness," in *9th EAI International Conference on Digital Forensics & Cyber Crime*, 2017, pp. 1–13.

[14] A. R. Ikuesan, S. A. Razak, H. S. Venter, and M. Salleh, "Polychronicity tendency-based online behavioral signature," *Int. J. Mach. Learn. Cybern.*, vol. 10, no. 8, pp. 2103–2118, 2019, doi: 10.1007/s13042-017-0748-7.

[15] I. R. Adeyemi, S. A. Razak, and M. Salleh, "Personality-Print on the Internet : Understanding Online Behavior," pp. 1–17, 2013.

[16] S. M. Makura, H. S. Venter, R. A. Ikuesan, V. R. Kebande, and N. M. Karie, "Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020, pp. 200–205, doi: 10.1109/ICIoT48696.2020.9089494.

[17] I. R. Adeyemi, "A New Heuristic Algorithm for Identification of User Initiated Request in HTTP Traffic for User Identification," pp. 1–2.

[18] I. R. Adeyemi, S. A. Razak, M. Salleh, and H. S. Venter, "Observing consistency in online communication patterns for user re-identification," *PLoS One*, vol. 11, no. 12, pp. 1–27, 2016, doi: 10.1371/journal.pone.0166930.

[19] D. Ellison, H. Venter, and A. Ikuesan, "An Improved Ontology for Knowledge Management in Security and Digital Forensics," in *European Conference on Cyber Warfare and Security*, 2017, pp. 725--733.

[20] B. Kitchenham, "Procedure for undertaking systematic reviews," *Comput. Sci. Depart-ment, Keele Univ. Natl. ICT Aust. Ltd (0400011T. 1), Jt. Tech. Rep.*, 2004.

[21] A. Al-Dhaqm, S. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," *IEEE Access*, p. 1, 2020, doi: 10.1109/ACCESS.2020.3008696.

[22] A. Al-Dhaqm *et al.*, "Categorization and Organization of Database Forensic Investigation Processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020, doi: 10.1109/access.2020.3000747.

[23] A. Al-Dhaqm, S. A. Razak, S. H. Othman, A. Nagdi, and A. Ali, "A generic database forensic investigation process model," *J. Teknol.*, vol. 78, no. 6–11, 2016, doi: 10.11113/jt.v78.9190.

[24] O. M. Fasan and M. Olivier, "Reconstruction in database forensics," in *IFIP International Conference on Digital Forensics*, 2012, pp. 273–287.

[25] H. Q. Beyers, "Database forensics: Investigating compromised database management systems." University of Pretoria, 2014.

[26] R. Susaimanickam, "A workflow to support forensic database analysis." Murdoch University, 2012.

[27] O. M. Fasan and M. S. Olivier, "On Dimensions of Reconstruction in Database Forensics.," in *WDFIA*, 2012, pp. 97–106.

[28] J. Yoon, D. Jeong, C. Kang, and S. Lee, "Forensic investigation framework for the document store NoSQL DBMS: MongoDB as a case study," *Digit. Investig.*, vol. 17, pp. 53–65, 2016.

[29] H. K. Khanuja and D. S. Adane, "A framework for database forensic analysis," *Comput. Sci. Eng.*, vol. 2, no. 3, p. 27, 2012.

[30] M. S. Olivier, "On metadata context in database forensics," *Digit. Investig.*, vol. 5, no. 3–4, pp. 115–123, 2009.

[31] D. Wong and K. Edwards, "System and method for investigating a data operation performed on a database." Google Patents, Dec. 29, 2005.

[32] P. M. Wright, "Oracle database forensics using LogMiner," in *June 2004 Conference, SANS Institute*, 2005, pp. 1–39.

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

[34] M. Malmgren, "An infrastructure for database tamper detection and forensic analysis," *Bachelor's Thesis, Uni¬ versity Arizona, Tucson*, 2007.

[35] D. Litchfield, "Oracle forensics part 4: Live response," *NGSSoftware Insight Secur. Res. (NISR), Next Gener. Secur. Softw. Ltd., Sutt.*, 2007.

[36] G. T. Lee, S. Lee, E. Tsomko, and S. Lee, "Discovering methodology and scenario to detect covert database system," in *Future Generation Communication and Networking (FGCN 2007)*, 2007, vol. 2, pp. 130–135.

[37] D. Litchfield, "Oracle forensics part 1: Dissecting the redo logs," *NGSSoftware Insight Secur. Res. (NISR), Next Gener. Secur. Softw. Ltd, Sutt.*, 2007.

[38] D. Litchfield, "Oracle forensics part 2: Locating dropped objects," *NGSSoftware Insight Secur. Res. Publ. Next Gener. Secur. Softw.*, 2007.

[39] D. Litchfield, "Oracle forensics part 5: Finding evidence of data theft in the absence of auditing," *NGSSoftware Insight Secur. Res. (NISR), Next Gener. Secur. Softw. Ltd, Sutt.*, 2007.

[40] D. Litchfield, "Oracle forensics part 6: Examining undo segments, flashback and the oracle recycle bin," *NGSSoftware Insight Secur. Res. Publ. Next Gener. Secur. Softw.*, 2007.

[41] D. Litchfield, "Oracle forensics part 7: using the Oracle system change number in forensic investigations," *Insight Secur. Res. Publ. NGSSoftware*, 2008.

[42] K. Fowler, *SQL server forenisc analysis*. Pearson Education, 2008.

[43] K. E. Pavlou and R. T. Snodgrass, "Forensic analysis of database tampering," *ACM Trans. Database Syst.*, vol. 33, no. 4, pp. 1–47, 2008.

[44] A. Basu, "Forensic tamper detection in SQL server," *Retrieved form http//www. sqlsecurity. com/chipsblog/archivedposts*, 2006.

[45] D. Lee, J. Choi, and S. Lee, "Database forensic investigation based on table relationship analysis techniques," in *2009 2nd International Conference on Computer Science and Its Applications, CSA 2009*, 2009, p. 5404235.

[46] P. Frühwirt, M. Huber, M. Mulazzani, and E. R. Weippl, "InnoDB database forensics," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 386, pp. 1028–1036, 2010, doi: 10.1109/AINA.2010.152.

[47] F. Fatima, "Detecting database attacks using computer forensics tools," *Dept. Comput. Sci., Texas A&M Univ. Corpus Christi, Corpus Christi, TX, USA, Tech. Rep*, 2011.

[48] H. Beyers, M. Olivier, and G. Hancke, "Assembling metadata for database forensics," in *IFIP International Conference on Digital Forensics*, 2011, pp. 89–99.

[49] N. Son, K. Lee, S. Jeon, H. Chung, S. Lee, and C. Lee, "The method of database server detection and investigation in the enterprise environment," in *FTRA International Conference on Secure and Trust Computing, Data Management, and Application*, 2011, pp. 164–171.

[50] H. Beyers, M. S. Olivier, and G. P. Hancke, "An approach to examine the Metadata and Data of a database Management System by making use of a forensic comparison tool.," 2011.

[51] S. Tripathi and B. B. Meshram, "Digital evidence for database tamper detection," 2012.

[52] S. Jeon, J. Bang, K. Byun, and S. Lee, "A recovery method of deleted record for SQLite database," *Pers. Ubiquitous Comput.*, vol. 16, no. 6, pp. 707–715, 2012.

[53] P. D. Abhonkar and A. Kanthe, "Enriching forensic analysis process for tampered data in database," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 5, pp. 5078–5085, 2012.

[54] K. E. Pavlou and R. T. Snodgrass, "Dragoon: An information accountability system for high-performance databases," in *2012 IEEE 28th International Conference on Data Engineering*, 2012, pp. 1329–1332.

[55] P. Frühwirt, P. Kieseberg, S. Schrittwieser, M. Huber, and E. Weippl, "Innodb database forensics: Reconstructing data manipulation queries from redo logs," in *2012 Seventh International Conference on Availability, Reliability and Security*, 2012, pp. 625–633.

[56] H. Beyers, M. S. Olivier, and G. P. Hancke, "Arguments and Methods for Database Data Model Forensics.," in *WDFIA*, 2012, pp. 139–149.

[57] H. K. Khanuja and D. Adane, "Forensic analysis of databases by combining multiple evidences," *Int. J. Comput. Technol.*, vol. 7, no. 3, pp. 654–663, 2013.

[58] K. E. Pavlou and R. T. Snodgrass, "Generalizing database forensics," *ACM Trans. Database Syst.*, vol. 38, no. 2, pp. 1–43, 2013.

[59] O. M. Adedayo and M. S. Olivier, "On the completeness of reconstructed data for database forensics," in *International Conference on Digital Forensics and Cyber Crime*, 2012, pp. 220–238.

[60] P. P. Gawali and S. R. Gupta, "Forensic Analysis Algorithm: By using the Tiled Bitmap with Audit Log Mechanism," *Int. J. Comput. Appl.*, vol. 63, no. 11, 2013.

[61] B. Wu, M. Xu, H. Zhang, J. Xu, Y. Ren, and N. Zheng, "A recovery approach for SQLite history recorders from YAFFS2," in *Information and Communication Technology-EurAsia Conference*, 2013, pp. 295–299.

[62] J.-H. Choi, D. W. Jeong, and S. Lee, "The method of recovery for deleted record in Oracle Database," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 23, no. 5, pp. 947–955, 2013.

[63] M. Xu *et al.*, "A metadata-based method for recovering files and file traces from YAFFS2," *Digit. Investig.*, vol. 10, no. 1, pp. 62–72, 2013.

[64] P. P. Gawali and D. S. R. Gupta, "Database tampering and detection of data fraud by using the forensic scrutiny technique," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 2, pp. 439–446, 2013.

[65] P. Frühwirt, P. Kieseberg, S. Schrittwieser, M. Huber, and E. Weippl, "InnoDB database forensics: Enhanced reconstruction of data manipulation queries from redo logs," *Inf. Secur. Tech. Rep.*, vol. 17, no. 4, pp. 227–238, 2013.

[66] M. Xu *et al.*, "A Reconstructing Android User Behavior Approach based on YAFFS2 and SQLite.," *J. Comput.*, vol. 9, no. 10, pp. 2294–2302, 2014.

[67] H. Khanuja and S. S. Suratkar, "Role of metadata in forensic analysis of database attacks," in *2014 IEEE International Advance Computing Conference (IACC)*, 2014, pp. 457–462.

[68] W. K. Hauger and M. S. Olivier, "The role of triggers in database forensics," in *2014 Information Security for South Africa*, 2014, pp. 1–7.

[69] P. Frühwirt, P. Kieseberg, K. Krombholz, and E. Weippl, "Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations," *Digit. Investig.*, vol. 11, no. 4, pp. 336–348, 2014.

[70] O. M. Adedayo, "Reconstruction in database forensics." University of Pretoria, 2015.

[71] H. K. Khanuja and D. S. Adane, "Forensic analysis for monitoring database transactions," in *International Symposium on Security in Computing and Communication*, 2014, pp. 201–210.

[72] J. Wagner, A. Rasin, and J. Grier, "Database forensic analysis through internal structure carving," *Digit. Investig.*, vol. 14, pp. S106–S115, 2015.

[73] O. M. Adedayo and M. S. Olivier, "Ideal log setting for database forensics reconstruction," *Digit. Investig.*, vol. 12, pp. 27–40, 2015.

[74] J. O. Ogutu, "A Methodology To Test The Richness Of Forensic Evidence Of Database Storage Engine: Analysis Of MySQL Update Operation In InnoDB And MyISAM Storage Engines." University of Nairobi, 2016.

[75] A. Aldhaqm, S. Abd Razak, S. H. Othman, A. Ali, and A. Ngadi, "Conceptual investigation process model for managing database forensic investigation knowledge," *Res. J. Appl. Sci. Eng. Technol.*, vol. 12, no. 4, pp. 386–394, 2016.

[76] J. Wagner, A. Rasin, T. Malik, K. Heart, H. Jehle, and J. Grier, "Database forensic analysis with DBCarver," 2017.

[77] A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a database forensic metamodel (DBFM)," *PLoS One*, vol. 12, no. 2, 2017, doi: 10.1371/journal.pone.0170793.

[78] A. Al-Dhaqm *et al.*, "CDBFIP: Common database forensic investigation processes for Internet of Things," *IEEE Access*, vol. 5, pp. 24401–24416, 2017.

[79] A. Al-Dhaqm, S. Razak, and S. H. Othman, "Model derivation system to manage database forensic investigation domain knowledge," in *2018 IEEE Conference on Application, Information and Network Security (AINS)*, 2018, pp. 75–80.

[80] R. Bria, A. Retnowardhani, and D. N. Utama, "Five stages of database forensic analysis: A systematic literature review," in *2018 International Conference on Information Management and Technology (ICIMTech)*, 2018, pp. 246–250.

[81] H. Choi, S. Lee, and D. Jeong, "Forensic Recovery of SQL Server Database: Practical Approach," *IEEE Access*, vol. 9, pp. 14564–14575, 2021.

[82] R. L. Delfanti *et al.*, "No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title," *N. Engl. J. Med.*, vol. 372, no. 2, pp. 2499–2508, 2018, doi: 10.1056/nejmoa1407279.

[83] D. Litchfield, "Oracle forensics part 3: Isolating evidence of attacks against the authentication mechanism, March 2007," *NGSSoftware Insight Secur. Res. Publ.*

[84] J. Azemović and D. Mušić, "Efficient model for detection data and data scheme tempering with purpose of valid forensic analysis," 2009.

[85] R. SNODGRASS, S. YAO, and C. COLLBERG, "Tamper Detection in Audit Logs," *Proc. 2004 VLDB Conf.*, pp. 504–515, 2004, doi: 10.1016/b978-012088469-8/50046-2.

[86] M. S. D. Chopade, S. S. Bere, M. N. B. Kasar, and M. A. V Moholkar, "SQL Query Recommendation Using Collaborative

Query Log: A Survey," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 2, no. 11, pp. 3715–3721.

[87] J. Yoon and S. Lee, "A method and tool to recover data deleted from a MongoDB," *Digit. Investig.*, vol. 24, pp. 106–120, 2018.

[88] A. Al-Dhaqm *et al.*, "Database forensic investigation process models: A review," *IEEE Access*, vol. 8, pp. 48477–48490, 2020, doi: 10.1109/ACCESS.2020.2976885.

[89] W. K. Hauger and M. S. Olivier, "The state of database forensic research," in *2015 Information Security for South Africa (ISSA)*, 2015, pp. 1–8.

[90] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 3–8, 2017.

[91] A. Al-Dhaqm, S. Abd Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A Review of Mobile Forensic Investigation Process Models," *IEEE Access*, vol. 8, pp. 173359–173375, 2020.

[92] M. W. Burnette, "Forensic Examination of a RIM (BlackBerry) Wireless Device June, 2002," *URL https//www. rh-law. com/ediscovery/Blackberry. pdf*, 2002.

[93] J. Grand, "pdd: memory imaging and forensic analysis of palm OS devices," 2002.

[94] S. Willassen, "Forensics and the GSM mobile telephone system," *Int. J. Digit. Evid.*, vol. 2, no. 1, pp. 1–17, 2003.

[95] B. Mellars, "Forensic examination of mobile phones," *Digit. Investig.*, vol. 1, no. 4, pp. 266–272, 2004.

[96] S. Willassen, "Forensic analysis of mobile phone internal memory," in *IFIP International Conference on Digital Forensics*, 2005, pp. 191–204.

[97] F. Casadei, A. Savoldi, and P. Gubian, "Forensics and SIM cards: an Overview," *Int. J. Digit. Evid.*, vol. 5, no. 1, pp. 1–21, 2006.

[98] P. M. Mokhonoana and M. S. Olivier, "Acquisition of a Symbian smart phone's content with an on-phone forensic tool," in *Proceedings of the Southern African Telecommunication Networks and Applications Conference*, 2007, vol. 8.

[99] K. Kim, D. Hong, K. Chung, and J.-C. Ryou, "Data acquisition from cell phone using logical approach," *Proc. world Acad. Sci. Eng. Technol.*, vol. 26, 2007.

[100] M. Al-Zarouni, "Introduction to mobile phone flasher devices and considerations for their use in mobile phone forensics," 2007.

[101] I. M. Baggili, R. Mislan, and M. Rogers, "Mobile phone forensics tool testing: A database driven approach."

[102] W. Jansen and R. Ayers, "Guidelines on cell phone forensics (NIST Special Publication 800-101)." Gaithersburg, MD: US Dept of Commerce Technology Administration National …, 2007.

[103] M. Breeuwsma, M. De Jongh, C. Klaver, R. Van Der Knijff, and M. Roeloffs, "Forensic data recovery from flash memory," *Small Scale Digit. Device Forensics J.*, vol. 1, no. 1, pp. 1–17, 2007.

[104] J. Luck and M. Stokes, "An integrated approach to recovering deleted files from NAND flash data."

[105] W. Jansen, A. Delaitre, and L. Moenner, "Overcoming impediments to cell phone forensics," in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 2008, p. 483.

[106] J. Zdziarski, *iPhone forensics: recovering evidence, personal data, and corporate assets*. " O'Reilly Media, Inc.," 2008.

[107] A. Distefano and G. Me, "An overall assessment of mobile internal acquisition tool," *Digit. Investig.*, vol. 5, pp. S121–S127, 2008.

[108] S. Danker, R. Ayers, and R. P. Mislan, "Hashing Techniques for Mobile Device Forensics," *Stress*, vol. 6, no. 4f16334e774b5c, p. 77bebd7fb998797dd, 2009.

[109] A. Savoldi and P. Gubian, "Issues in Symbian S60 platform forensics," *J Commun Comput*, vol. 6, no. 3, pp. 16–22, 2009.

[110] A. Savoldi, P. Gubian, and I. Echizen, "A comparison between windows mobile and Symbian S60 embedded forensics," in *2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009, pp. 546–550.

[111] X. Yu, L.-H. Jiang, H. Shu, Q. Yin, and T.-M. Liu, "A process model for forensic analysis of Symbian smart phones," in *International Conference on Advanced Software Engineering and Its Applications*, 2009, pp. 86–93.

[112] D. Y. Kao, M. C. Chen, W. Y. Wu, J. S. Lin, C. H. Chen, and F. Tsai, "Drone forensic investigation: DJI spark drone as a case study," *Procedia Comput. Sci.*, vol. 159, pp. 1890–1899, 2019, doi: 10.1016/j.procs.2019.09.361.

[113] F. Dellutri, V. Ottaviani, D. Bocci, G. F. Italiano, and G. Me, "Data reverse engineering on a smartphone," in *2009 International Conference on Ultra Modern Telecommunications & Workshops*, 2009, pp. 1–8.

[114] C. Shaoyan, H. Xianwei, and L. Ming, "Research of mobile forensic software system based on windows mobile," in *2009 international conference on wireless networks and information systems*, 2009, pp. 366–369.

[115] D. Irwin and R. Hunt, "Forensic information acquisition in mobile networks," in *2009 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, 2009, pp. 163–168.

[116] C. Klaver, "Windows Mobile advanced forensics," *Digit. Investig.*, vol. 6, no. 3–4, pp. 147–167, 2010.

[117] R. Berte, F. Dellutri, A. Grillo, A. Lentini, G. Me, and V. Ottaviani, "Fast smartphones forensic analysis results through mobile internal acquisition tool and forensic farm," *Int. J. Electron. Secur. Digit. Forensics*, vol. 2, no. 1, pp. 18–28, 2009.

[118] J. Lessard and G. Kessler, "Android Forensics: Simplifying Cell Phone Examinations.," 2010.

[119] E. Casey, M. Bann, and J. Doyle, "Introduction to windows mobile forensics." Elsevier, 2010.

[120] H.-C. Chu, L.-W. Wu, H.-M. Yu, and J. H. Park, "Digital Trails Discovering of a GPS Embedded Smart Phone-Take Nokia N78 Running Symbian S60 Ver 3.2 for Example," in *FTRA International Conference on Secure and Trust Computing, Data Management, and Application*, 2011, pp. 41–49.

[121] D. Quick and M. Alzaabi, "Forensic analysis of the android file system yaffs2," 2011.

[122] A. M. de L. Simão, F. C. Sícoli, L. P. de Melo, F. E. G. de Deus, and R. T. de Sousa Júnior, "Acquisition and analysis of digital evidencein android smartphones," 2011.

[123] W.-S. Chun and D.-W. Park, "A study on the forensic data extraction method for sms, photo and mobile image of google android and windows mobile smart phone," in *International Conference on Hybrid Information Technology*, 2012, pp. 654–663.

[124] J. Park, H. Chung, and S. Lee, "Forensic analysis techniques for fragmented flash memory pages in smartphones," *Digit. Investig.*, vol. 9, no. 2, pp. 109–118, 2012.

[125] W. Jansen and R. Ayers, "Guidelines on PDA forensics," *NIST Spec. Publ.*, vol. 800, p. 72, 2004.

[126] M. Bader and I. Baggili, "iPhone 3GS forensics: Logical analysis using apple iTunes backup utility," 2010.

[127] I. Pooters, "Full user data acquisition from Symbian smart phones," *Digit. Investig.*, vol. 6, no. 3–4, pp. 125–135, 2010.

[128] F. Rehault, "Windows mobile advanced forensics: An alternative to existing tools," *Digit. Investig.*, vol. 7, no. 1–2, pp. 38–47, 2010.

[129] S. Morrissey and T. Campbell, *iOS Forensic Analysis: for iPhone, iPad, and iPod touch*. Apress, 2011.

[130] M. I. Husain, I. Baggili, and R. Sridhar, "A simple cost-effective framework for iPhone forensic analysis," in *International Conference on Digital Forensics and Cyber Crime*, 2010, pp. 27–37.

[131] G. Grispos, T. Storer, and W. B. Glisson, "A comparison of forensic evidence recovery techniques for a windows mobile smart phone," *Digit. Investig.*, vol. 8, no. 1, pp. 23–36, 2011.

[132] T. Vidas, C. Zhang, and N. Christin, "Toward a general collection methodology for Android devices," *Digit. Investig.*, vol. 8, pp. S14–S24, 2011.

[133] S. Maus, H. Höfken, and M. Schuba, "Forensic analysis of geodata in android smartphones," 2011.

[134] Y. Lai, C. Yang, C. Lin, and T. Ahn, "Design and

implementation of mobile forensic tool for android smart phone through cloud computing," in *International Conference on Hybrid Information Technology*, 2011, pp. 196–203.

[135] M. Zhu, "Mobile Cloud Computing: implications to smartphone forensic procedures and methodologies." Auckland University of Technology, 2011.

[136] J. Lee and D. Hong, "Pervasive forensic analysis based on mobile cloud computing," in *2011 Third international conference on multimedia information networking and security*, 2011, pp. 572–576.

[137] V. L. L. Thing and T.-W. Chua, "Symbian smartphone forensics: Linear bitwise data acquisition and fragmentation analysis," in *Computer applications for security, control and system engineering*, Springer, 2012, pp. 62–69.

[138] F. N. Dezfouli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani, and S. bin Shamsuddin, "Volatile memory acquisition using backup for forensic investigation," in *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 2012, pp. 186–189.

[139] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digit. Investig.*, vol. 9, pp. S24–S33, 2012.

[140] A. Goel, A. Tyagi, and A. Agarwal, "Smartphone forensic investigation process model," *Int. J. Comput. Sci. Secur.*, vol. 6, no. 5, pp. 322–341, 2012.

[141] J. Sylve, A. Case, L. Marziale, and G. G. Richard, "Acquisition and analysis of volatile memory from android devices," *Digit. Investig.*, vol. 8, no. 3–4, pp. 175–184, 2012.

[142] P. Andriotis, G. Oikonomou, and T. Tryfonas, "Forensic analysis of wireless networking evidence of android smartphones," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012, pp. 109–114.

[143] M. Al Marzougy, I. Baggili, and A. Marrington, "Blackberry playbook backup forensic analysis," in *International Conference on Digital Forensics and Cyber Crime*, 2012, pp. 239–252.

[144] A. Mylonas, V. Meletiadis, B. Tsoumas, L. Mitrou, and D. Gritzalis, "Smartphone forensics: A proactive investigation scheme for evidence acquisition," in *IFIP International Information Security Conference*, 2012, pp. 249–260.

[145] A. Mahajan, M. S. Dahiya, and H. P. Sanghvi, "Forensic analysis of instant messenger applications on android devices," *arXiv Prepr. arXiv1304.4915*, 2013.

[146] N. S. Thakur, "Forensic analysis of WhatsApp on Android smartphones," 2013.

[147] A. Ariffin, C. DOorazio, K.-K. R. Choo, and J. Slay, "ios forensics: How can we recover deleted image files with timestamp in a forensically sound manner?," in *2013 International conference on availability, reliability and security*, 2013, pp. 375–382.

[148] X. Chang, X. Tang, and J. Wu, "Forensic research on data recovery of android smartphone," in *Proc. 2nd ICCSE*, 2013, p. 1188.

[149] E. S. Canlar, M. Conti, B. Crispo, and R. Di Pietro, "Windows mobile LiveSD forensics," *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 677–684, 2013.

[150] L. Gómez-Miralles and J. Arnedo-Moreno, "Analysis of the forensic traces left by airprint in apple ios devices," in *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, 2013, pp. 703–708.

[151] A. Mylonas, V. Meletiadis, L. Mitrou, and D. Gritzalis, "Smartphone sensor data as digital evidence," *Comput. Secur.*, vol. 38, pp. 51–75, 2013.

[152] P. Dibb and M. Hammoudeh, "Forensic data recovery from android os devices: an open source toolkit," in *2013 European Intelligence and Security Informatics Conference*, 2013, p. 226.

[153] M. Zheng, M. Sun, and J. C. S. Lui, "Droid analytics: a signature based analytic system to collect, extract, analyze and associate android malware," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, pp. 163–171.

[154] S. Zhang and L. Wang, "Forensic analysis of social networking application on iOS devices," in *Sixth International Conference on Machine Vision (ICMV 2013)*, 2013, vol. 9067, p. 906715.

[155] C.-P. Chang, C.-T. Chen, T.-H. Lu, I.-L. Lin, P. Huang, and H.-S. Lu, "Study on constructing forensic procedure of digital evidence on smart handheld device," in *2013 International Conference on System Science and Engineering (ICSSE)*, 2013, pp. 223–228.

[156] W. Takahashi, R. Sasaki, and T. Uehara, "Development and Evaluation of Guideline Total Support System for Evidence Preservation by Using an Android Phone," in *2013 IEEE 37th Annual Computer Software and Applications Conference Workshops*, 2013, pp. 21–26.

[157] Y.-C. Tsai and C.-H. Yang, "Physical forensic acquisition and pattern unlock on Android smart phones," in *Future information communication technology and applications*, Springer, 2013, pp. 871–881.

[158] C.-W. Song, J.-H. Lim, K.-Y. Chung, K.-W. Rim, and J.-H. Lee, "Fast data acquisition with mobile device in digital crime," in *IT Convergence and Security 2012*, Springer, 2013, pp. 711–717.

[159] F. C. Dancer, D. A. Dampier, J. M. Jackson, and N. Meghanathan, "A theoretical process model for smartphones," in *Advances in computing and information technology*, Springer, 2013, pp. 279–290.

[160] C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," *Digit. Investig.*, vol. 11, no. 3, pp. 201–213, 2014.

[161] Y. Yang, Z. Zu, and G. Sun, "Historical data recovery from Android devices," in *Future Information Technology*, Springer, 2014, pp. 251–257.

[162] K. Paul, "'Generic process model for Android smartphones live memory forensics," *Fac. Comput. Inf. Manag. KCA Univ., Nairobi, Kenya, Tech. Rep*, pp. 1–87, 2014.

[163] Q. Do, B. Martini, and K.-K. R. Choo, "A forensically sound adversary model for mobile devices," *PLoS One*, vol. 10, no. 9, p. e0138449, 2015.

[164] D. M. Sai, N. Prasad, and S. Dekka, "The forensic process analysis of mobile device," *Int. J. Comput. Sci. Inf. Technol*, vol. 6, no. 5, pp. 4847–4850, 2015.

[165] V. R. Kebande, N. M. Karie, and S. Omeleze, "A mobile forensic readiness model aimed at minimizing cyber bullying," *Int. J. Comput. Appl.*, vol. 140, no. 1, pp. 28–33, 2016.

[166] M. Faheem, N.-A. Le-Khac, and T. Kechadi, "Toward a new mobile cloud forensic framework," in *2016 sixth international conference on innovative computing technology (INTECH)*, 2016, pp. 736–742.

[167] A. Azfar, K.-K. R. Choo, and L. Liu, "An android social app forensics adversary model," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 5597–5606.

[168] A. Ali, S. Abd Razak, S. H. Othman, A. Mohammed, and F. Saeed, *A Metamodel for Mobile Forensics Investigation Domain*, vol. 12, no. 4. 2017.

[169] C.-T. Huang, H.-J. Ko, Z.-W. Zhuang, P.-C. Shih, and W. Shiuh-Jeng, "Mobile forensics for cloud storage service on ios systems," in *2018 International Symposium on Information Theory and Its Applications (ISITA)*, 2018, pp. 178–182.

[170] M. Goel and V. Kumar, "Layered framework for mobile forensics analysis," 2019.

[171] F. G. Hikmatyar and B. Sugiantoro, "Digital forensic analysis on Android smartphones for handling cybercrime cases," *IJID (International J. Informatics Dev.*, vol. 7, no. 2, pp. 64–67, 2018.

[172] A. Fukami and K. Nishimura, "Forensic analysis of water damaged mobile devices," *Digit. Investig.*, vol. 29, pp. S71–S79, 2019.

[173] D. K. Sharma, K. Kwatra, and M. Manwani, "Smartphone security and forensic analysis," in *Research Anthology on Securing Mobile Technologies and Applications*, IGI Global, 2021, pp. 1–22.

[174] P. Sharma, D. Arora, and T. Sakthivel, "Mobile cloud forensic readiness process model for cloud-based mobile applications," *Int. J. Digit. Crime Forensics*, vol. 12, no. 3, pp. 58–76, 2020.

[175] P. Sharma, D. Arora, and T. Sakthivel, "Mobile Cloud Correlated Digital Forensic Process Model based on UML Design," *Int. J.*, vol. 9, no. 4, 2020.

[176] A. Fukami, R. Stoykova, and Z. Geradts, "A new model for forensic data extraction from encrypted mobile devices," *Forensic Sci. Int. Digit. Investig.*, vol. 38, p. 301169, 2021.
[177] X. Zhang, C. Z. Liu, K.-K. R. Choo, and J. A. Alvarado, "A design science approach to developing an integrated mobile app forensic framework," *Comput. Secur.*, vol. 105, p. 102226, 2021.
[178] I. A. Alnajjar and M. Mahmuddin, "The Enhanced Forensic Examination and Analysis for Mobile Cloud Platform by Applying Data Mining Methods.," *Webology*, vol. 18, no. SI01, pp. 47–74, 2021.
[179] T. Müller and S. M. FROST, "In Applied Cryptography and Network Security, Jacobson M, Locasto M, Mohassel P, Safavi-Naini R." Springer, 2013.
[180] N. Al Barghouthy and A. Marrington, "A comparison of forensic acquisition techniques for android devices: a case study investigation of orweb browsing sessions," in *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*, 2014, pp. 1–4.
[181] B. L. Schatz, "A visual approach to interpreting NAND flash memory," *Digit. Investig.*, vol. 11, no. 3, pp. 214–223, 2014.
[182] K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, "Mobile Forensic Data Analysis: Suspicious Pattern Detection in Mobile Evidence," *IEEE Access*, vol. 6, pp. 59705–59727, 2018.
[183] R. Wilson and H. Chi, "A framework for validating aimed mobile digital forensics evidences," in *Proceedings of the ACMSE 2018 Conference*, 2018, pp. 1–8.
[184] H. Alatawi, K. Alenazi, S. Alshehri, S. Alshamakhi, M. Mustafa, and A. Aljaedi, "Mobile Forensics: A Review," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, 2020, pp. 1–6.
[185] A. M. Alashjaee, N. Almolhis, and M. Haney, "Mobile Malware Forensic Review: Issues and Challenges," in *Advances in Security, Networks, and Internet of Things*, Springer, 2021, pp. 367–375.
[186] B. Bernardo and V. Santos, "Mobile Device Forensics Investigation Process: A Systematic Review," *Handb. Res. Cyber Crime Inf. Priv.*, pp. 256–288, 2021.
[187] I. R. Adeyemi, S. Abd Razak, and N. A. N. Azhan, "A review of current research in network forensic analysis," *Int. J. Digit. Crime Forensics*, vol. 5, no. 1, pp. 1–26, 2013.
[188] I. Adeyemi, S. Razak, and N. Azhan, "Identifying critical features for network forensics investigation perspectives," *Int. J. Comput. Sci. Inf. Secur.*, vol. 10, no. Issue 9, p. 108, 2012.
[189] M. Lagrasse, A. Singh, H. Munkhondya, A. Ikuesan, and H. Venter, "Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism," in *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 2020, pp. 296–305, doi: 10.34190/ICCWS.20.045.
[190] H. Munkhondya, A. R. Ikuesan, and H. S. Venter, "A Case for a Dynamic Approach to Digital Forensic Readiness in an SDN Platform," in *International Conference on Cyber Warfare and Security*, 2020, pp. 584–XVIII.
[191] G. S. Chhabra and P. Singh, "Distributed Network Forensics Framework: A Systematic Review," *Int. J. Comput. Appl.*, vol. 119, no. 19, 2015.
[192] Y. Tang and T. E. Daniels, "A simple framework for distributed forensics," in *25th IEEE International Conference on Distributed Computing Systems Workshops*, 2005, pp. 163–169.
[193] T. Hong, Z. Tao, J. Qi, and Z. Jianbo, "A distributed framework for forensics based on the content of network transmission," in *2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control*, 2011, pp. 852–855.
[194] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digit. Investig.*, vol. 7, no. 1–2, pp. 14–27, 2010.
[195] T. Gebhardt and H. P. Reiser, "Network forensics for cloud computing," in *IFIP International Conference on Distributed Applications and Interoperable Systems*, 2013, pp. 29–42.
[196] "On A Reference Model of Distributed Cooperative Network, Forensics System."
[197] R. Wei, "A framework of distributed agent-based network forensics system," in *Digital Forensic Research Workshop*, 2004, pp. 11–13.
[198] W. Ren and H. Jin, "Distributed agent-based real time network intrusion forensics system architecture design," in *19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers)*, 2005, vol. 1, pp. 177–182.
[199] D. Wang, T. Li, S. Liu, J. Zhang, and C. Liu, "Dynamical network forensics based on immune agent," in *Third International Conference on Natural Computation (ICNC 2007)*, 2007, vol. 3, pp. 651–656.
[200] B. Endicott-Popovsky, D. A. Frincke, and C. A. Taylor, "A Theoretical Framework for Organizational Network Forensic Readiness.," *JCP*, vol. 2, no. 3, pp. 1–11, 2007.
[201] S. Ngobeni, H. Venter, and I. Burke, "A forensic readiness model for wireless networks," in *IFIP International Conference on Digital Forensics*, 2010, pp. 107–117.
[202] E. S. Pilli, R. C. Joshi, and R. Niyogi, "A framework for network forensic analysis," in *International Conference on Advances in Information and Communication Technologies*, 2010, pp. 142–147.
[203] R. Ammann, "Network forensic readiness: a bottom-up approach for IPv6 networks." Auckland University of Technology, 2012.
[204] S. Ngobeni, H. S. Venter, and I. Burke, "The modelling of a digital forensic readiness approach for wireless local area networks," 2012.
[205] M. Mulazzani, M. Huber, and E. Weippl, "Social network forensics: Tapping the data pool of social networks," in *Eighth Annual IFIP WG*, 2012, vol. 11, p. 1Ű20.
[206] D. Avasthi, "Network Forensic Analysis with Efficient Preservation for SYN Attack," *Int. J. Comput. Appl.*, vol. 46, no. 24, pp. 17–22, 2012.
[207] A. Al-Mahrouqi, S. Abdalla, and T. Kechadi, "Network forensics readiness and security awareness framework," 2014.
[208] C. Liu, A. Singhal, and D. Wijesekera, "Creating integrated evidence graphs for network forensics," in *IFIP International Conference on Digital Forensics*, 2013, pp. 227–241.
[209] M. Thapliyal, A. Bijalwan, N. Garg, and E. S. Pilli, "A generic process model for botnet forensic analysis," 2013.
[210] E. Saari and A. Jantan, "A framework to increase the accuracy of collected evidences in network forensic by integrating IDS and firewall mechanisms," in *Proceedings of the International Conference on Systems, Control and Informatics. Snort. Retrieved December*, 2013, vol. 21, p. 2016.
[211] S. Parate, S. M. Nirkhi, and R. V Dharaskar, "Application of Network Forensics for Detection of Web Attack using Neural Network," *networks*, vol. 4, p. 12, 2013.
[212] A. R. Amran and A. Saad, "An evidential network forensics analysis model with adversarial capability and layering," in *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 2014, pp. 1–9.
[213] S. Mittal and R. Singh, "Securing Network Flow Using Network Forensics," *Int. J.*, vol. 6, no. 5, 2016.
[214] P. Kaur, A. Bijalwan, R. C. Joshi, and A. Awasthi, "Network forensic process model and framework: an alternative scenario," in *Intelligent Communication, Control and Devices*, Springer, 2018, pp. 493–502.
[215] S. J. Ngobeni and H. S. Venter, "Design of a wireless forensic readiness model (WFRM)," 2009.
[216] A. Kyaw, B. Cusack, and R. Lutui, "Digital Forensic Readiness In Wireless Medical Systems," in *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, 2019, pp. 1–6.
[217] R. Lu and L. Li, "Research on Forensic Model of Online Social Network," in *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, 2019, pp. 116–119.
[218] D. Saputra and I. Riadi, "Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 1, pp. 66–73, 2019.
[219] H. Arshad, A. Jantan, G. K. Hoon, and I. O. Abiodun, "Formal

knowledge model for online social network forensics," *Comput. Secur.*, vol. 89, p. 101675, 2020.

[220] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Futur. Gener. Comput. Syst.*, vol. 110, pp. 91–106, 2020.

[221] R. N. Malvankar and A. Jain, "EnNetForens: An Efficient Proactive Approach For Network Forensic," in *2021 International Conference on Communication, Control and Information Sciences (ICCISc)*, 2021, vol. 1, pp. 1–4.

[222] S. Parate and S. M. Nirkhi, "A Review of Network Forensics Techniques for the analysis of Web Based attack," *Int. J. Adv. Comput. Res.*, vol. 2, no. 4, p. 114, 2012.

[223] M. J. Islam, M. Mahin, A. Khatun, B. C. Debnath, and S. Kabir, "Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach," in *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, 2019, pp. 1–6.

[224] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for internet of things (iot)," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016, pp. 356–362.

[225] V. R. Kebande, N. M. Karie, and H. S. Venter, "Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures," in *2017 1st International Conference on Next Generation Computing Applications (NextComp)*, 2017, pp. 54–60.

[226] E. Oriwoh and P. Sant, "The forensics edge management system: A concept and design," in *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, 2013, pp. 544–550.

[227] S. Perumal, N. M. Norwawi, and V. Raman, "Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology," in *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, 2015, pp. 19–23.

[228] A. Nieto, R. Rios, and J. Lopez, "A methodology for privacy-aware IoT-forensics," in *2017 IEEE Trustcom/BigDataSE/ICESS*, 2017, pp. 626–633.

[229] N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "IoT forensic: bridging the challenges in digital forensic and the Internet of Things," in *International Conference on Internet of Things, Big Data and Security*, 2017, vol. 2, pp. 315–324.

[230] T. Zia, P. Liu, and W. Han, "Application-specific digital forensics investigative model in internet of things (iot)," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–7.

[231] E. Al-Masri, Y. Bai, and J. Li, "A fog-based digital forensics investigation framework for IoT systems," in *2018 IEEE International Conference on Smart Cloud (SmartCloud)*, 2018, pp. 196–201.

[232] F. Bouchaud, G. Grimaud, and T. Vantroys, "IoT Forensic: identification and classification of evidence in criminal investigations," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1–9.

[233] H. Chi, T. Aderibigbe, and B. C. Granville, "A framework for IoT data acquisition and forensics analysis," in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 5142–5146.

[234] V. R. Kebande *et al.*, "Towards an integrated digital forensic investigation framework for an IoT-based ecosystem," in *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 2018, pp. 93–98.

[235] S. Sathwara, N. Dutta, and E. Pricop, "IoT Forensic A digital investigation framework for IoT systems," in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2018, pp. 1–4.

[236] J. Song and D. Park, "Preemptive Cyber Response Strategy and IoT Forensic Evidence," 2018.

[237] V. R. Kebande, N. M. Karie, and H. S. Venter, "Functional requirements for adding digital forensic readiness as a security component in iot environments," 2018.

[238] M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework," in *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, 2017, pp. 1–6.

[239] S. Li, K.-K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, "IoT forensics: Amazon echo as a use case," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6487–6497, 2019.

[240] T. Bakhshi, "Forensic of Things: Revisiting Digital Forensic Investigations in Internet of Things," in *2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*, 2019, pp. 1–8.

[241] P. Harris, J. Ma, I. Salas, and I. Sanchez, "DFRWS IoT Forensic Challenge Report 3," in *Digital Forensic Education*, Springer, 2020, pp. 43–60.

[242] S. Kang, S. Kim, and J. Kim, "Forensic analysis for IoT fitness trackers and its application," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 564–573, 2020.

[243] V. R. Kebande, P. P. Mudau, R. A. Ikuesan, H. S. Venter, and K.-K. R. Choo, "Holistic digital forensic readiness framework for IoT-enabled organizations," *Forensic Sci. Int. Reports*, vol. 2, p. 100117, 2020.

[244] N. Scheidt and M. Adda, "Identification of IoT devices for forensic investigation," in *2020 IEEE 10th International Conference on Intelligent Systems (IS)*, 2020, pp. 165–170.

[245] N. Scheidt and M. Adda, "Framework of confidence values during digital forensic investigation processes," *WSEAS Trans. Syst. Control*, vol. 15, pp. 228–234, 2020.

[246] A. Hilgenberg, T. Q. Duong, N.-A. Le-Khac, and K.-K. R. Choo, "Digital Forensic Investigation of Internet of Thing Devices: A Proposed Model and Case Studies," in *Cyber and Digital Forensic Investigations*, Springer, 2020, pp. 31–49.

[247] A. Akinbi and T. Berry, "Forensic Investigation of Google Assistant," *SN Comput. Sci.*, vol. 1, no. 5, pp. 1–10, 2020.

[248] B. K. Sharma, M. Hachem, V. P. Mishra, and M. J. Kaur, "Internet of Things in Forensics Investigation in Comparison to Digital Forensics," in *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, Springer, 2020, pp. 672–684.

[249] J. M. C. Gómez, J. C. Mondéjar, J. R. Gómez, and J. M. Martínez, "Developing an IoT forensic methodology. A concept proposal," *Forensic Sci. Int. Digit. Investig.*, vol. 36, p. 301114, 2021.

[250] N. H. N. Zulkipli and G. B. Wills, "An Exploratory Study on Readiness Framework in IoT Forensics," *Procedia Comput. Sci.*, vol. 179, pp. 966–973, 2021.

[251] J. A. Raman and V. Varadharajan, "HoneyNetCloud Investigation Model, A Preventive Process Model for IoT Forensics.," *Ingénierie des Systèmes d'Information*, vol. 26, no. 3, 2021.

[252] A. Hambouz, Y. Shaheen, and M. Ababneh, "An Internet Of Things (IoT) Forensics Model Using Third-Party Logs-Vault," in *International Conference on Data Science, E-learning and Information Systems 2021*, 2021, pp. 143–146.

[253] P. M. Shakeel, S. Baskar, H. Fouad, G. Manogaran, V. Saravanan, and C. E. Montenegro-Marin, "Internet of things forensic data analysis using machine learning to identify roots of data scavenging," *Futur. Gener. Comput. Syst.*, vol. 115, pp. 756–768, 2021.

[254] M. A. Saleh, S. H. Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Common Investigation Process Model for Internet of Things Forensics," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2021, pp. 84–89.

[255] N. A. Almolhis, "Development of an Advanced Privacy-Aware IoT Forensics Process Model." University of Idaho, 2021.

[256] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: Challenges and approaches," in *9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing*, 2013, pp. 608–615.

[257] S. Zawoad and R. Hasan, "Faiot: Towards building a forensics

aware eco system for the internet of things," in *2015 IEEE International Conference on Services Computing*, 2015, pp. 279–284.

[258] H. F. Atlam, E. E.-D. Hemdan, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Internet of Things Forensics: A Review," *Internet of Things*, p. 100220, 2020.

[259] A. ALJAHDALI, H. ALDISSI, S. BANAFEE, S. SOBAHI, and W. NAGRO, "IoT Forensic models analysis," *Rom. J. Inf. Technol. Autom. Control*, vol. 31, no. 2, pp. 21–34, 2021.

[260] P. M. Shakeel, S. Baskar, H. Fouad, G. Manogaran, V. Saravanan, and C. E. Montenegro-Marin, "Internet of things forensic data analysis using machine learning to identify roots of data scavenging," *Futur. Gener. Comput. Syst.*, 2020.

[261] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues," *IEEE Commun. Surv. Tutorials*, 2020.

[262] G. Surange and P. Khatri, "IoT Forensics: A Review on Current Trends, Approaches and Foreseen Challenges," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2021, pp. 909–913.

[263] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, and G. B. Wills, "Security, Cybercrime and Digital Forensics for IoT," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, Springer, 2020, pp. 551–577.

[264] A. Ghosh, K. Majumder, and D. De, "A Systematic Review of Digital, Cloud and IoT Forensics," *The" Essence" Netw. Secur. An End-to-End Panor.*, pp. 31–74, 2021.

[265] T. Janarthanan, M. Bagheri, and S. Zargari, "IoT Forensics: An Overview of the Current Issues and Challenges," *Digit. Forensic Investig. Internet Things Devices*, pp. 223–254, 2021.

[266] N. Almolhis, A. M. Alashjaee, and M. Haney, "Requirements for IoT Forensic Models: A Review," *Adv. Secur. Networks, Internet Things*, pp. 355–366, 2021.

[267] M. A. Hossain and B. Al-Athwari, "Blockchain-Based IoT Forensics: Challenges and State-of-the-Art Frameworks," *Artif. Intell. Blockchain Futur. Cybersecurity Appl.*, p. 361.

[268] P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama, and B. B. Bastaki, "The complexity of internet of things forensics: A state-of-the-art review," *Forensic Sci. Int. Digit. Investig.*, vol. 38, p. 301210, 2021.

[269] D. Ellison, R. A. Ikuesan, and H. S. Venter, "Ontology for Reactive Techniques in Digital Forensics," *2019 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2019*, pp. 83–88, 2019, doi: 10.1109/AINS47559.2019.8968696.

[270] E. Casey, G. Back, and S. Barnum, "Leveraging CybOX??? to standardize representation and exchange of digital forensic information," *Digit. Investig.*, vol. 12, no. S1, pp. S102–S110, 2015, doi: 10.1016/j.diin.2015.01.014.

[271] D. Ellison, A. R. Ikuesan, and H. Venter, "Description Logics and Axiom Formation for a Digital Forensics Ontology," in *European Conference on Cyber Warfare and Security*, 2019, pp. 742--XIII.

[272] A. Singh, A. Ikuesan, and H. Venter, "A Context-Aware Trigger Mechanism for Ransomware Forensics," in *International Conference on Cyber Warfare and Security*, 2019, pp. 629–XV.

[273] A. Al-Dhaqm *et al.*, "CDBFIP: Common Database Forensic Investigation Processes for Internet of Things," *IEEE Access*, vol. 5, 2017, doi: 10.1109/ACCESS.2017.2762693.