Systematic Review

A Comprehensive Literature Review on Volatile Memory Forensics

Ishrag Hamid * and M. M. Hafizur Rahman

Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia; mhrahman@kfu.edu.sa
* Correspondence: 223002631@student.kfu.edu.sa

Abstract: Through a systematic literature review, which is considered the most comprehensive way to analyze the field of memory forensics, this paper investigates its development through past and current methodologies, as well as future trends. This paper systematically starts with an introduction to the key issues and a notable agenda of the research questions. Appropriate inclusion and exclusion criteria were then developed, and a deliberate search strategy was adopted to identify primary research studies aligned with the research question. The paper goes into specific details of six different memory categories, notably volatile memory, interpreting their advantages and the tactics used to retrieve the data. A detailed comparison with existing reviews and other relevant papers is made, forming a broader and wider picture of the research. The discussion summarizes the main findings, particularly the rise of more complex and advanced cyber threats and the necessity of more effective forensic methods for their investigation. This review pinpoints the possibilities for future study with the purpose of staying ahead in the evolving technological landscape. This overview is undoubtedly an essential resource for professionals and researchers working in digital forensics. It allows them to stay competent and provides enough insight into the current trends while marking the future direction in digital forensics methodology.

Keywords: memory forensics; forensic tools; forensic techniques; cybersecurity; volatile memory; technological advancements; digital investigations

check for updates

Citation: Hamid, I.; Rahman, M.M.H. A Comprehensive Literature Review on Volatile Memory Forensics. *Electronics* **2024**, *13*, 3026. https://doi.org/10.3390/electronics13153026

Academic Editor: Myung-Sup Kim

Received: 8 May 2024
Revised: 21 June 2024
Accepted: 28 June 2024
Published: 31 July 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Memory forensics is now an integral component of digital investigations and cybersecurity. Mainly, RAM and other volatile memories are analyzed in depth for gathering valuable data, which is significant in identifying cyber threats, system invasion, and some unusual existing digital anomalies [1]. The high instability of this memory is just another characteristic indicating loss of data when the system is turned off, which leads to the necessity to carefully retrieve information within a certain time frame [2]. The digital environment and cyber area constantly evolve through the implementation of new technologies and the modernization of hackers, which calls for the application of memory forensics. It has the extremely significant purpose of recovering evidence that cannot be unveiled from traditional media storage, providing a snapshot of the system's condition at a certain point in time [3]. This could include the names of processes and open files that were running, network connections, encryption keys, etc., all of which are primary components in search history that could lead to a security event.

A thorough review of the available body of knowledge through a systematic literature review offers the possibility to integrate already existing empirical results, point out deficits in scientific research, and design the path for further research in this field [4]. It is more of a psychological transformation process that renders a systematic literature review (SLR) in memory forensics to better understand the advancement of forensic techniques, tools, and methodologies, as well as the challenges faced by scientists and practitioners [5]. The entire process aims at compiling a general review based not only on current knowledge but also on providing an outline for future research in the field [6]. The next sections of this SLR will outline the methodology for paper selection, discuss how memory forensics is considered, compare this review with the existing literature, discuss related work, and finally present the findings, future research directions, and a conclusion highlighting the most important aspects [7]. The research questions followed by this study aim at identifying the most appropriate methods in memory forensics, unveiling the effect of technological advances on forensic techniques, and examining the ethical and legal issues involved.

Overview of Sections

The SLR system extensively analyzed the improvements in memory forensics in the realm of cybersecurity [8]. It began by meticulously choosing which papers to study. A checklist of what should be included and excluded was created, and a comprehensive plan for locating the required information was developed [7]. Our goal was to have a good collection of the literature. In the first section, the concept of memory forensics recognizes the crucial role of volatile memory and familiar forensic approaches to build a solid base for deeper comprehension [9]. A thematic comparative analysis of other review articles is done to point out the novel parts and methodological differences in this SLR, illustrating its position among the existing body of the literature. The main research contributions section provides an extensive view of foundational research breakthroughs that have changed the face of the field, building up a historical context for its present condition [10]. The SLR concludes with a discussion of the compendium of the gathered research results, addressing the initial research questions and highlighting trends and challenges that enrich the storyline of the present condition of memory forensics [11]. The future work section will indicate paths for the next wave of research, and the concluding statement captures the essence of the SLR, highlighting the vital role of memory forensics in cybersecurity and the need for continuous academic commitment to this field. Our research questions are as follows:

1. How successful are the current methods and devices of memory forensics, and in which areas do they differ in terms of precision, speed, and usability?
   The aim of this question is to assess whether the memory forensic tools currently used for investigative purposes are effective. The pros and cons of these tools will be evaluated to determine how effective they are for different types of investigations.
2. What is the role in the development of memory forensic methods of breakthroughs in hardware and software technology, and what challenges have emerged with them?
   The aim of this question is to understand the evolution of memory forensic techniques, considering the new challenges that may arise due to increasing amounts of data and advances in encryption.
3. What ethics and laws are involved in memory forensics, and how are these being considered in ongoing research and practice?

This question probes into the ethical and legal issues in memory forensics, including privacy concerns and the admissibility of electronic evidence, and how these issues are being handled in the field.

2. Methodology for Literature Selection

Selecting which articles to incorporate into this memory forensics review holds great significance. We want to ensure that the review is based on relevant and high-quality research.

2.1. Inclusion and Exclusion Criteria

This systematic literature review (SLR) on memory forensics will include and exclude papers to ensure the review focuses solely on relevant and high-quality research [12]. The inclusion criteria involve papers that address memory forensics directly, with main topics including forensic analysis techniques, memory acquisition tools, or methodologies for examining volatile memory [13]. Furthermore, to reflect modern trends and occurrences, only papers published within designated timeframes, commonly within the last five to ten years, are covered [6]. Additionally, the literature search targets peer-reviewed journal articles and papers from reputable conferences to ensure the authenticity and accuracy of the research [14]. Papers must contain empirical evidence, such as case studies, experiments, or quantitative analysis, and be written in English to maintain consistency and accessibility for a broad audience.

In contrast, the exclusion criteria are adapted to filter out papers that are not relevant or of insufficient quality [8]. Documents that do not have memory forensics as the primary topic or do not discuss memory forensics directly are excluded [15]. Moreover, papers that are purely theoretical without any empirical validation of the proposed approach or methods are considered unsuitable [16]. The review also rejects research that does not meet academic standards, such as those lacking a solid methodology or having severe design flaws [17]. Similar research, namely studies with the same outcome or data, is eliminated to avoid redundancy; additionally, papers not written in English are excluded unless they are of exceptional relevance and a summary or translation is available.

2.2. Search Strategy

The systematized search strategy of this systematic literature review (SLR) on memory forensics is carefully designed to facilitate the identification of the existing literature on memory forensics and enable the implementation of a systematic and comprehensive search [10]. The first step in the strategy execution is the selection of relevant databases known for their extensive collections of academic and research papers in computer science and cybersecurity [3]. Key databases include IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink, among others. Only databases containing peer-reviewed articles of high quality are selected, as these are most relevant to the subject matter. The development of important keywords is a critical point of the plan [9]. The language employed incorporates a combination of keywords and phrases to cover the variety of topics associated with this subject. Phrases like "volatile Memory Analysis", "Memory Dump", "RAM Forensics", "Live Memory Capture", and "Digital Forensics" are used to encompass different types of memory forensics techniques in general [4]. A literature review and input from expert consultants helped finalize a list that covers all related topics.

Boolean operators play a crucial role in enhancing search effectiveness. Words like "AND", "OR", and "NOT" help combine keywords and phrases to refine the search results [11]. For instance, searching for "memory forensics AND volatile memory analysis OR RAM forensics" will find papers about memory forensics and either volatile memory analysis or RAM forensics. Selecting which parts of the databases to search in, such as titles, summaries, and keywords, can help make the search more precise [15]. This ensures that the results are closely linked to the research questions and objectives of the study. Furthermore, filters can be employed to seek out recent investigations, typically from the previous 5 to 10 years, to ensure the review encompasses the latest advancements and trends in the subject. Overall, the search plan aims to uncover a large number of relevant studies on memory forensics while maintaining a focus on the key themes [18]. By being meticulous, this method establishes a strong basis for a comprehensive and informed review of the current research in memory forensics.

2.3. Paper Selection Process

The selection of papers for this research on memory forensics demands great attention and adherence to strict criteria. It is done in multiple stages to ensure that only the best and most important papers are included. The first step involves a broad exploration using a specific approach. The collection of papers is examined by reviewing their titles and abstracts. This screening aims to eliminate any papers not related to memory forensics [19]. During the first stage of research evaluation, we consider whether the research aligns with our research questions, focuses on memory forensics, and incorporates essential terminology related to the field. Papers failing to meet these criteria will not be taken into consideration [17]. The papers that pass the first round are then thoroughly reviewed. During this stage, the documents are thoroughly reviewed to ensure they adhere to the specified guidelines [16]. The review team examines the papers to determine if they are adequately researched, relevant to the subject, contribute to the field, and are supported by strong evidence. Documents that do not meet the inclusion and exclusion criteria will not be considered in the review.

In the text review stage, it is common for reviewers to have differing perspectives on which papers should be added or removed. The reviewers discuss with each other to reach a consensus on the decision. If an agreement cannot be reached, another reviewer will be asked to give their opinion and help decide what should be done [13]. The papers that make it through all the steps of the selection process are included in the SLR for further analysis. This final group of papers is the most important and highest quality, and they will be the main focus of the review.

Measures are implemented throughout the paper selection process to ensure that the evaluation is truthful and dependable [16]. The steps involve clarity and organization, noting reasons for paper selections, and ensuring the process is fair and repeatable. By carefully selecting papers in multiple steps, the SLR ensures that the final papers chosen will provide a strong base for a thorough and thoughtful analysis of the current research in memory forensics.

2.4. PRISMA Statement and Flow Diagram

The memory analysis research reviewed in this paper aligns with the provided guidelines for identifying, screening, and selecting studies on memory forensics. The search was conducted in IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink, using keywords such as “cloud computing”, “cloud storage”, “security challenges”, “issues”, and “security threats”. Some of the phrases used to search for the topic include “volatile memory analysis”, “RAM forensic”, “live memory acquisition”, and “digital forensic”. Specifically, the inclusion criteria for this review were set as follows: (1) the studies include aspects of memory forensics as a primary focus; (2) the studies were published in 2013 or after the year of the last research; (3) the research was published in English; (4) only academic articles from peer-reviewed journals or conference proceedings were considered. The review excluded theoretical papers or articles without empirical evidence, duplicated papers, and those that failed to meet academic requirements, such as studies with weak methodological development or poor study design. Papers unrelated to memory analysis were filtered out to enhance the scope and credibility of the review.

The authors ensured a very rigorous process of study selection. First, the literature was searched on SCOPUS, Web of Science, PubMed, Google Scholar, and other sources, and 1200 records were initially selected. Records were then culled by deleting duplicates, leaving a total of 1000 records from which articles were screened by their titles and/or abstracts. Through this screening process, 700 records were excluded as they did not meet the eligibility criteria. Thus, 200 potentially relevant articles containing full texts were identified, to which the authors’ selection criteria were applied. Despite this, the remaining 150 articles were considered and excluded due to factors such as little relevance, lack of data or empirical analysis, methodological issues, and repetition. After the initial screening and extraction of relevant data for 107 studies, 50 studies were made the basis for the final qualitative and quantitative synthesis, faithfully reflecting the current state of research in the field of memory forensics. Figure 1 shows the PRISMA 2020 Flow Diagram.

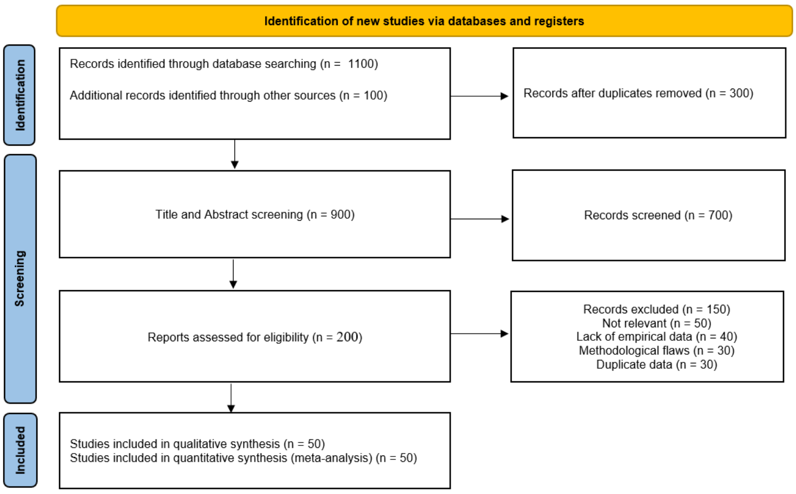
Identification of new studies via databases and registers
Identification
Records identified through database searching (n = 1100)
Additional records identified through other sources (n = 100)
Records after duplicates removed (n = 300)
Screening
Title and Abstract screening (n = 900)
Records screened (n = 700)
Reports assessed for eligibility (n = 200)
Records excluded (n = 150)
Not relevant (n = 50)
Lack of empirical data (n = 40)
Methodological flaws (n = 30)
Duplicate data (n = 30)
Included
Studies included in qualitative synthesis (n = 50)
Studies included in quantitative synthesis (meta-analysis) (n = 50)

Figure 1. PRISMA2020 flow diagram.

3. Background

Memory forensics plays a critical role in digital investigations by analyzing the volatile memory in computers to uncover evidence of cybercrime or unauthorized activities. This aspect of forensics is crucial in contemporary cybersecurity as it enables the retrieval of volatile data that are otherwise inaccessible [20]. This includes details about programs running, internet connections, and potentially harmful software in the computer's memory. One of the primary concerns in memory forensics is the rapid and potential change or disappearance of data [21]. Information stored on a hard drive remains intact, while data in memory are vulnerable to being lost or altered when the power is off. This means that forensic investigators need to act quickly and accurately to gather memory dumps before important evidence disappears. Capturing and analyzing memory dumps is a complex task that requires special tools and skills [22]. Investigators need to understand how the operating system and memory work to interpret the results correctly.

With the ever-changing landscape of cybersecurity threats, memory forensics becomes more challenging. Modern computer viruses and advanced threats are designed to operate exclusively within the computer's memory, minimizing their presence on the hard drive [23]. This type of malware, called fileless malware, is hard to detect using traditional forensic methods. Memory forensics is crucial for identifying and understanding these types of threats. Additionally, cloud computing and virtualization have introduced new challenges to memory forensics. Investigators now need to consider the intricacies of analyzing memory in virtual environments, where multiple virtual machines share the same physical resources.

3.1. Types of Memory

The importance of memory in the computer world cannot be overstated, as it is essential for storing and processing data. There are two main types of memory: volatile and non-volatile.

Volatile Memory: Volatile memory, such as Random Access Memory (RAM) and cache memory, requires power to retain data. It allows for quick data storage and processing but loses data when the power is off, posing challenges for preserving evidence during investigations [24,25].

Non-Volatile Memory: Non-volatile memory retains data without power, making it suitable for long-term storage. Examples include Hard Disk Drives (HDDs), Solid-State Drives (SSDs), and flash memory used in USB drives and memory cards. This type of memory is crucial for preserving data over time [15].

The distinction between volatile and non-volatile memory is significant in digital forensics. Volatile memory requires specialized techniques for effective analysis due to its transient nature, while non-volatile memory is typically the focus of traditional disk forensics. Understanding these differences is essential for forensic investigators in modern computing environments [26].

3.2. Volatile Memory Overview

Volatile memory, such as RAM, is crucial for the functioning of computers. It serves as the intermediate storage medium for data and code that the processor utilizes for quick reads. This type of memory is characterized by its high transmission speed and capability to retrieve required information within a short time interval, performing significantly better compared to non-volatile options like hard drives and solid-state drives [27]. However, the downside is that when the PC is switched off or interrupted, all previously stored information is lost.

RAM, a type of volatile memory, is significant in computing systems because it can read and write data approximately 100,000 times faster than flash memory. This level of speed directly impacts the performance of programs and the smooth operation of the OS, contributing to overall system efficiency [28]. The quick disappearance of data from volatile memory when the system power is switched off provides secure protection, as sensitive information, such as passwords or encryption keys, is erased, reducing the risk of unauthorized access. RAM allows the processor to directly access any memory component and quickly locate information, even if it is stored in different memory segments [28]. This random access capability is essential for efficient multitasking, enabling more complex applications to frequently access various data points. Furthermore, mass storage supports and enforces the resource allocation policy used by the computing system, efficiently distributing memory resources to each process or application to ensure smooth operation.

The primary reason for choosing volatile memory is its low latency, especially compared to non-volatile memories [16]. Fast data access is crucial for both sensitive applications and real-time processing where delays are unacceptable. RAM is designed for storing temporary data and calculation results, and it can dynamically read or write to memory. This makes RAM suitable for scenarios where permanent data storage is unnecessary, such as caching or buffering [11]. However, the complexity of maintaining volatile memory patterns makes the design of memory modules sophisticated [24]. Overall, the advantages of volatile memory, including its speedy performance and temporary nature, facilitate efficient and secure computing operations.

Volatile memory is a fundamental component of computing hardware and is available in several types, each with unique properties for specific tasks. Among MOS memory types, Dynamic RAM (DRAM) and Static RAM (SRAM) are the most popular and widely used. DRAM, the most common type of RAM, is found in low-cost and high-density systems, making it possible to build high-capacity computers and other devices [29]. DRAM stores data in capacitors where charge drains over time, necessitating periodic refreshes to maintain the data. This refresh process may introduce some delays, affecting access times compared to other types of memory. Despite this, DRAM is often preferred as the main memory in computing systems due to its cost-effectiveness and desired performance [10]. Conversely, SRAM is much faster and more stable than DRAM, as it does not require refreshing. SRAM uses bistable latching circuitry to store each bit, allowing it to process, read, and write operations more efficiently [2]. However, the increased speed comes at a higher financial and spatial cost, as SRAM cells occupy more physical space on a chip than DRAM cells. Due to its larger size and higher cost per bit, SRAM is frequently used in small amounts as cache memory for processors, where speed is the primary concern.

3.3. Memory Forensic Techniques

Memory forensics is a crucial method in cybersecurity and digital investigations. It examines the temporary memory in a computer to find evidence and understand how the system was acting during an incident [3]. The first step is to capture the information in the computer's memory using special tools like FTK Imager, DumpIt, and WinPmem, without altering the data. This step is essential for preserving the evidence safely and intact [4]. After capturing the information, the memory is usually turned into a memory image, which is an exact copy of the temporary memory that can be analyzed [6].

Studying running programs is an important part of memory investigation. It includes examining active programs, their memory locations, and other details to identify any suspicious or malicious activities. This method of memory forensics helps investigators analyze and interpret the information from a computer's temporary memory to gain valuable insights into the system's activities at the time of the incident. Figure 2 illustrates the different ways to analyze digital memories for investigations. It shows the relationship between process virtual memory, physical memory, and hard drive paged data, highlighting how data can belong to the process, another process, or be unallocated.

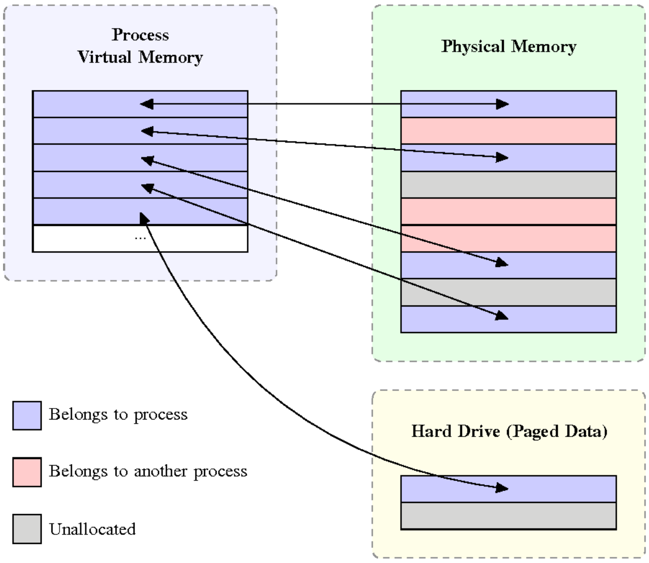

Figure 2. Difference ways to analyze digital memories for investigations.

Regarding the specificity of the accuracy and practicality of the methods and devices used in the context of the first research question, it is necessary to highlight certain parameters and indicators that reveal the effectiveness of existing memory forensic technologies. The measure of precision in memory forensics may involve the following aspects: the accuracy of malware identification, the number of false positive and false negative conclusions, and the strength to detect different types of threats. For instance, Volatility and Rekall are two of the tools that have been assessed based on their results in accurately capturing memory dumps and detecting malicious processes. Various studies report over 90 percent accuracy of these tools in ideal conditions, yet their performance in real-life scenarios depends on the characteristics of the threats and the abilities of the forensic experts.

Another important set of measures includes false positive and false negative rates; the former should be low to avoid the problem of legitimate activities being labeled as malicious, whereas the latter should also be low so that the tool does not fail to recognize all malicious activity. Usability, on the other hand, consists of parameters such as tool ease of use, time to learn the tool, compatibility with other tools, and the time needed to accomplish typical forensic tasks. Tools that are easy to navigate and accompanied by comprehensive resources on usage ease the work of both experienced and relatively inexperienced forensic analysts. Software with the best support, easy-to-learn, and easy-to-use interfaces includes FTK Imager and Autopsy.

Usability also includes considerations of integration with other forensic tools for tasks such as network analysis or disk forensics. Integration is a significant advantage as it allows various features of investigative work to be connected and analyzed without needing to switch between systems and applications to gather results. Furthermore, the usability and speed of a tool in executing forensic work are crucial; tools capable of processing large memory dumps and offering efficient results with minimal intervention from the forensic analyst are always preferred in forensic work.

4. Analyzing Existing Literature Reviews

4.1. Comparative Analysis of Existing Literature Reviews: Background and Scope

The relevance of the topic in the memory forensics review corresponds to the overall importance of the field and key issues in cybersecurity and digital investigations. Similarly, Strandberg et al. [1] focus on automotive digital forensics, noting its indispensability in today's automobile applications. Coronel et al. [2] apply cyber forensics from a client-oriented approach, which can be useful for businesses and individuals who have become targets of cybercriminal activities. Expanding the field of memory forensics to recommend potential sub-domains that can be considered promising but not covered in the review can provide updated and comprehensive information on the topic.

The analyzed memory forensics review also presents a clear goal, addressing memory analysis methods and their relevance in digital investigations. Ishrag et al. [3] express their goals in improving malware detection techniques through memory analysis. Further specifying the objectives in future reviews can provide a clearer idea for subsequent studies.

4.2. Methodology

The memory forensics review is conducted with a deep literature search covering various approaches and tools used in memory analysis. Similar to the study by Manral et al. [6], the authors perform a comprehensive literature search focusing on the challenges and solutions in cloud forensics. More inclusive results could be attained by liberalizing the criteria for selecting sources, which could enrich systematic reviews in the future. The articles included in the memory forensics review apply a range of selection criteria, but more stringent criteria could be beneficial. Alharbi, Weber-Jahnke, and Traore [30] present a clear balanced model containing both proactive and reactive activities. Adopting stricter criteria for selecting studies would help filter out poor-quality and irrelevant ones.

The number of analytical levels in the memory forensics review is high, allowing for a detailed analysis of certain tools and methods. Bai et al. [7] provide substantial insights into approaches for analyzing additional elements present in cloud forensics. Using advanced data analysis methods could further improve the quality and comprehensiveness of future reviews.

4.3. Findings

The use of memory forensics in the analysis of computer evidence is a relatively new idea, and the innovative discoveries in this review are encouraging as they show improvements in methodologies for memory analysis. Recent advancements in malware detection, such as those covered by Ishrag et al. [3], highlight the significance of memory forensics. Future reviews should also emphasize significant findings to demonstrate state-of-the-art advancements in the field.

Current trends in technological domains are discussed in the context of memory forensic reviews, particularly the coverage of technological trends. The same authors discuss issues connected with more sophisticated cyber threats in Pandey et al. [31]. Focusing more on the most current technologies would ensure that reviews remain up-to-date with new developments, enhancing their relevance.

The usefulness of case studies in memory forensics will be illustrated through a couple of examples. Coronel et al. [2] use case studies to elucidate the use of forensic tools effectively. Future reviews should emphasize practical examples and ensure that conclusive findings are applicable.

4.4. Gaps in Literature

The purpose of identifying limitations is effectively addressed in the memory forensics review section, where existing drawbacks and problem areas in the current approaches are indicated. Manral et al. [6] also discuss the challenges associated with forensic investigation in cloud computing environments. Extending projections to the less researched domain of future reviews would be beneficial in presenting a broader view of the area. Gaps in the field are mentioned in the memory forensics review section, with a suggested list of directions that require additional study. Ghosh, Majumder, and De [13] stress the importance of more effective and innovative approaches to tackling complex cyber threats. Particular concern was expressed in suggesting further research in novel areas as a way of extending existing review horizons.

5. Main Research Contributions

This section examines pertinent studies in the field, summarizing their key findings on volatility memory forensics and outlining potential mitigation based on our current knowledge, as presented in Table 1.

Table 1. An overview of the related work papers.

Paper	Key Finding	Limitation/Research Gap	Suggested Mitigation
Coronel et al. [2]	Trends in cyber forensics from a client perspective	Need for user-friendly forensic tools for non-technical users	Enhance collaboration among stakeholders
Ishrag et al. [3]	Advancements in malware artifact detection	Challenges in processing large memory dumps	Require automated tools for analysis
Alharbi, Weber-Jahnke, and Traore [30]	Efficiency of proactive in digital forensics	Difficulty in consistently adapting to evolving cyber-threats	Combine proactive and reactive methods
Maneli et al. [4]	3D crime scene reconstruction using immersive tech	Technical restrictions and privacy concerns	Standardization and validation of reconstruction methods
Hamid, Alabdulhay, and Hafizur Rahman [5]	Importance of volatility memory in forensics	Need for standard solutions for memory anomalies	Research and development in memory forensics
Manral et al. [6]	Challenges in cloud forensics	Data dispersion and jurisdiction issues in cloud computing	Collaboration between cloud providers and investigators
Bai et al. [7]	Complexities in cloud forensics	Difficulty in evidence gathering due to cloud complexity	Develop forensic tools specific to cloud architectures
Bahrum et al. [8]	Advances in face sketch recognition systems	Achieving high accuracy with different sketch styles	Further research to enhance system performance
Strandberg et al. [1]	Automotive digital forensics challenges and solutions	Complexity of automotive systems and data volatility	Develop specific forensic tools and address privacy concerns
Coronel et al. [2]	Trends in cyber forensics from a client perspective	Need for user-friendly forensic tools for non-technical users	Enhance collaboration among stakeholders
Alharbi, Weber-Jahnke, and Traore [30]	Efficiency of proactive in digital forensics	Difficulty in consistently adapting to evolving cyber-threats	Combine proactive and reactive methods
Maneli, et al. [4]	3D crime scene reconstruction using immersive tech	Technical restrictions and privacy concerns	Standardization and validation of reconstruction methods
Manral et al. [6]	Challenges in cloud forensics	Data dispersion and jurisdiction issues in cloud computing	Collaboration between cloud providers and investigators

Table 1. *Cont.*

Paper	Key Finding	Limitation/Research Gap	Suggested Mitigation
Bai et al. [7]	Complexities in cloud forensics	Difficulty in evidence gathering due to cloud complexity	Develop forensic tools specific to cloud architectures
Bahrum et al. [8]	Advances in face sketch recognition systems	Achieving high accuracy with different sketch styles	Further research to enhance system performance
Al-Dhaqm, Ghabban et al. [32]	Mobile forensic investigation process models	Rapid evolution of mobile devices and encryption	Develop adaptive frameworks and automatic data extraction tools
Lutta et al. [11]	Challenges in IoT forensics	Device interoperability and evolving IoT technologies	Intersectoral cooperation for accepted practices
Fernando et al. [12]	Mechanism of cyber forensic tools	Evolving challenges in cyber forensics like encryption	Interdisciplinary collaboration for tool enhancement
Ghosh, Majumder, and De [13]	Digital, cloud, and IoT forensics in network security	Managing vast data and variety of devices	Strategic plans for diverse cyber threats
Paul Joseph and Norman [15]	Ransomware detection using memory forensics	Limited methods in current memory forensic tools	Research for improved memory forensic tools
Gancedo et al. [16]	Reality monitoring in forensic practice	Limited reliability in legal proceedings	Research and standardized guidelines for reality monitoring
Chopade and Pachghare [17]	Database forensics over a decade	Need for more efficient solutions to complex database issues	Interdisciplinary collaboration and standardization
Azzery, Mulyanto, and Hidayat [33]	Memory forensics in digital crime detection	Handling encryption and anti-forensic methods	Enhance forensic tools and techniques
Ganesh, Venkatesh, and Prasad [34]	Forensics in cloud, IoT, AI and blockchain	Specific complexities in each sector	Utilize AI and blockchain for improved forensic practices
Al-Dhaqm, Siddique et al. [10]	Approaches in database forensic investigations	Gaps in current investigation models	Improve efficiency of investigation models
Sjöstrand et al. [35]	Tackling data volume issues in digital forensics	Difficulty in managing extensive data	Develop enhanced data management strategies
Pandey et al. [31]	Challenges in cyber security digital forensics	Need for standardized tools and collaboration	Enhance collaborative efforts across sectors
Case et al. [36]	Using Hooktracer for keystroke logger detection	Necessity for tools against keystroke loggers	Apply Hooktracer for effective malware detection
Nayerifard et al. [37]	Machine learning in digital forensics	Need for quality training data and adaptable algorithms	Focus on developing and refining ML techniques
Aly et al. (2019)	Security challenges in IoT frameworks	Evolving threats and need for comprehensive security	Continuous research and development in IoT security
Al-Dhaqm, Ghabban et al. [29]	State-of-the-art in digital forensics subdomains	Rapid technological advancements outpacing current methods	Interdisciplinary R&D and integration of AI and ML

5.1. Overview of Key Works

The study by Strandberg et al. [1] provides a comprehensive guide to the field of automotive digital forensics, focusing on identifying challenges and technologies for their solution. In addition, it critically analyzes the current state of research. It shows that automotive systems increase the complexity of forensic tasks and suggests advanced forensic techniques to handle issues such as data volatility and proprietary formats. The review emphasizes the necessity of conformity in forensic processes and the development of specific instruments for obtaining and investigating information from car systems. It also elaborates on the legal and ethical dilemmas of automotive forensics, highlighting the need to balance privacy concerns with investigative needs. Therefore, the review is a highly useful tool for researchers and professionals, enabling them to learn about the latest trends and opportunities for growth in automotive digital forensics.

A systematic review by Coronel et al. [2] investigates the adaptability of cyber forensics through a client-centered paradigm, focusing on individuals and companies affected by cybercrimes. It appraises the current traits, problems, and achievements in the field of digital evidence, regularly stressing the rising complexity and theories of cybercrime forensics. This paper offers a brief assessment of the need to develop user-friendly forensic tools and services that meet the needs of non-technical users while maintaining privacy and legal compliance during investigations. It also highlights the role of collaboration among cyber law enforcement authorities, forensic experts, and clients in elevating the quality of cyber forensic investigations. The article underscores the developments in digital forensics and technology and their adaptation to existing customer needs in the digital era, which demand ongoing changes and modernization.

The study by Hamid Riad et al. [3] examines recent developments in malware detection and memory forensics, as well as the analysis of artifacts. This positions memory forensics as a vital component in contemporary cybersecurity, addressing the inadequacies of traditional disk-based forensic techniques in detecting advanced malware. The study highlights the development of memory forensic techniques in response to evolving cybercriminal methods. It also describes the challenges faced by researchers and practitioners, such as processing large volumes of memory dumps and the need for automated tools to aid in the analysis process. Overall, the review outlines the significant role of memory forensics in enhancing malware detection and analysis capabilities.

The paper by Alharbi, Weber-Jahnke, and Traore [30] evaluates the techniques and approaches used in both proactive and reactive digital forensics investigations. It shows that a proactive stance in forensics is more efficient than reactive measures typically taken after an incident has occurred. The paper highlights a balanced approach incorporating both proactive and reactive techniques to improve digital forensics in light of ever-changing cyber threats. It also underscores the challenges of implementing such measures and the need for continued adaptability within the investigative field to keep up with changing technologies.

5.2. Comparative Analysis of Methods

A systematic literature review by Maneli et al. [4] reflects the trend of merging immersive technologies like virtual reality (VR) and augmented reality (AR) in 3D forensic crime kinetic reconstruction. It underlines that such technologies have the potential to improve the performance and reduce the operational time of crime scene investigations by offering a virtual and interactive setting. This article examines the obstacles related to incorporating these technologies, such as technical restrictions, privacy concerns, and the need for training forensic experts. It also reveals the necessity for standardization and validation of 3D reconstruction methods to ensure their reliability and admissibility in legal processes. Overall, the review shows that forensic science is poised for significant transformation by these advanced technologies, though their adoption is currently limited by several challenges that need to be addressed.

A systematic literature review by Ishrag et al. [5] investigates the current state of memory forensics, particularly in volatile memory, which is one of the most critical elements in the field. This review demonstrates why memory analysis is gaining increased importance for uncovering evidence that may not be available through traditional disk-based forensics, especially in malware investigations and Advanced Persistent Threat (APT) cases. The paper highlights the challenges faced by memory forensics, including the modification of memory structures, the time-consuming nature of forensic analysis, and the processing of large datasets. It emphasizes that maintaining standard solutions and methods is essential for the precision and credibility of memory anomaly detection. The review concludes that volatile memory forensics is exploring new horizons and dimensions in modern cybersecurity and digital forensic investigations, but there is a need for further research and development.

A systematic survey by Manral et al. [6] analyzes the complexities of cloud forensics, identifying unique difficulties associated with cloud computing architecture, such as data dispersion, multi-tenancy, and jurisdictional issues. The article reviews available solutions, including forensic data acquisition techniques, incident response strategies, and legal concerns. The manuscript points out future research directions, suggesting the advancement of methods, the automation of procedures, and collaboration between cloud service providers and investigators to enhance the effectiveness of cloud forensic investigations.

The paper by Bai et al. [7] examines the complexities of cloud forensics, focusing on forensic investigations in cloud environments. It highlights the intricacy of cloud infrastructures, which complicates evidence gathering and analysis, and stresses the need for forensic tools and techniques specifically designed for cloud architectures. The writing provides clear guidance on the legal and privacy implications of investigating in cloud environments, emphasizing the need for clear guidelines and international cooperation. The assessment underscores the importance of ongoing research and technological advancements to keep pace with the rapidly evolving landscape of cloud computing.

5.3. Thematic Categorization

A systematic review by Bahrum et al. [8] investigates the current state and advancements in face sketch recognition systems. These systems play a vital role in areas such as forensic investigation and security applications, as they are used to compare hand-drawn sketches and photographs. The discussion provides an elaborate overview of the different techniques and algorithms used in face sketch recognition, including feature extraction methods and machine learning approaches. Furthermore, the paper illustrates the challenges of attaining high accuracy, such as the variability in sketch styles and techniques. It also suggests directions for further research to improve the performance of these systems. In short, the review highlights the need for continuous development of face sketch recognition technology as the requirements of police and security units evolve.

A review by Dhaqm et al. [32] focuses on mobile forensics, emphasizing the growing need for forensic techniques as smartphones increasingly hold private and sensitive information. The paper describes the challenges in mobile forensics, including the diversity of mobile devices, encryption, and the rapid evolution of mobile technology. It assesses current process models, highlighting the importance of regulatory and adaptive frameworks as technology and legal circumstances change. The review also identifies existing gaps and suggests avenues for further research, such as developing tools for accurate and automated data extraction and processing. Ultimately, the paper underscores the importance of an appropriate investigation process model to enhance the trustworthiness and effectiveness of mobile crime scene analysis.

A paper by Lutta et al. [11] critically examines the intricate challenges associated with forensic investigations in the Internet of Things (IoT) ecosystem. It indicates that the diverse and interconnected world of IoT devices can complicate crime traceability. The research focuses on challenges such as channel variability, device interoperability, and the rapid evolution of forensic systems in the extensive IoT landscape. It calls for the design of advanced tools and mechanisms to address the upcoming transformations in IoT technology. The analysis also emphasizes the need for cooperation among industry, academia, and law enforcement to establish accepted practices and ensure IoT evidence is admissible in court. In summary, the paper highlights the problems in IoT forensics and advocates for concerted efforts to overcome these obstacles.

A paper by Fernando et al. [12] analyzes the functionality of cyber forensic tools and the challenges they face in the evolving digital sphere. It demonstrates the importance of these tools for finding and analyzing digital evidence. The paper emphasizes the need to enhance tools to address evolving challenges such as encryption, cloud computing, and increasingly complex cyber attacks. It advocates for collaboration among academia, industry, and law enforcement to improve and adapt cyber forensic tools.

A systematic review by Ghosh et al. [13] analyzes the relationship between digital, cloud, and IoT forensics in the context of network security. Investigating crimes in these interconnected areas presents unique challenges, such as managing vast amounts of information, dealing with a variety of devices, and requiring specialized tools and methods. The paper highlights the importance of creating strategies that can address the diverse cyber threats in digital, cloud, and IoT environments.

5.4. Innovations and Gaps

A review and analysis by Paul et al. [15] investigates how memory forensics can contribute to the fight against the rising threat of ransomware. It shows how memory forensics is crucial for finding and analyzing ransomware clues that cannot be detected through normal disk-based analysis. The paper discusses various methods of examining computer memory to uncover the workings of ransomware attacks, highlighting both the positive and negative aspects of these approaches. This underscores the need for continuous improvement in memory forensic tools to keep up with ransomware and enhance cybersecurity. In conclusion, the review demonstrates the significance of memory forensics in combating ransomware and calls for more research and collaboration in this area.

A paper by Gancedo et al. [16] investigates the effectiveness of reality monitoring in forensic science. It emphasizes the importance of distinguishing between actual events and imagined scenarios, which is crucial in legal matters, particularly in eyewitness testimony and false confessions. The research paper examines various studies to evaluate the reliability and utility of reality monitoring techniques in forensic applications. It suggests that while reality monitoring could be beneficial, further research and regulations are needed to improve its applicability in legal proceedings.

A paper by Chopade et al. [17] provides a comprehensive analysis of the developments and challenges in the field of database forensics over a decade. It critically examines the methodologies, tools, and techniques employed in database forensic investigations, highlighting progress made in addressing complex issues such as data recovery, log analysis, and tamper detection. The paper also identifies gaps in current research, emphasizing the need for more robust and efficient forensic solutions to cope with the increasing volume and complexity of data in modern databases. It underscores the importance of interdisciplinary collaboration and the development of standardized practices to advance the field of database forensics. Overall, the review serves as a valuable resource for researchers and practitioners seeking to understand the evolution and future directions of database forensic research.

5.5. Methodological Challenges

The paper by Azzery et al. [33] shows how memory forensics is becoming increasingly important for finding and analyzing data that can be used as evidence in cybercrime cases. The paper addresses the obstacles of analyzing memory, including handling encryption, anti-forensic methods, and constantly shifting memory data. It also emphasizes the need for continually enhancing forensic tools and techniques to stay ahead of evolving digital threats. In summary, the review highlights the critical role of memory forensics in aiding law enforcement and investigators in combating digital crime more effectively.

The paper by Ganesh et al. [34] delves into the intricacies of using cloud computing, the Internet of Things (IoT), artificial intelligence (AI), and blockchain technologies in forensic investigations and the obstacles they present. This highlights the specific requirements and complexities in examining various sectors, such as protecting data privacy in cloud forensics, handling multiple devices in IoT, addressing ethical considerations in AI, and ensuring transparency in blockchain. The article emphasizes the necessity of collaboration among various experts to devise effective solutions to ever-evolving cybercrimes. It shows that AI and blockchain can enhance forensic work in cloud and IoT systems.

The paper by Dhaqm et al. [32] investigates the use of models in tackling problems related to retrieving, scrutinizing, and presenting digital evidence from databases. The paper highlights the importance of having a well-organized and meticulous approach to investigating databases to ensure the evidence is admissible in court. It also identifies gaps in current models and recommends potential areas for future research to improve the efficiency of database forensic investigations. Overall, the review provides valuable insights into the use of databases in digital investigations, helping us understand the current methods and their utility.

The study by Sjöstrand et al. [35] discusses the growing challenge of handling large volumes of data in digital investigations. The article addresses the difficulty of managing extensive data in forensic investigations and offers solutions for this predicament. According to the review, there is a need for enhanced strategies for handling extensive data and verifying its validity to effectively address criminal cases. Continued research and development in this area are necessary to keep up with the evolving digital landscape and the increasing complexity of cybercrimes.

5.6. Emerging Technologies

The paper by Pandey et al. [31] investigates the increasing complexity of cyber threats and the difficulties in investigating them. The paper addresses issues surrounding the vast amount of data, its security in relation to cloud computing, and the importance of standardized rules and tools for data management. It stresses the need for academia, industry, and law enforcement to collaborate and continually adapt their methods to enhance digital forensics' effectiveness. The report highlights the critical role of digital forensics in protecting computers from cyber attacks and underscores the need for ongoing efforts to address emerging challenges in this area.

The study by Case et al. [36] focuses on the utilization of Hooktracer to strengthen cybersecurity by identifying and examining keystroke loggers stored in a computer's memory. This demonstrates the severity of keystroke loggers in stealing online information, highlighting the necessity for effective tools to detect and prevent this type of malware. The paper shows that Hooktracer is effective at detecting malicious keystroke-logging activities by analyzing memory evidence, making it a valuable tool for digital investigations and protection against cyber attacks.

The paper by Nayerifard et al. [37] explores the utilization of machine learning in digital forensics. According to the review, machine learning is playing an increasingly crucial role in expediting, improving accuracy, and automating forensic investigations, particularly when analyzing extensive and intricate digital information. The use of machine learning in digital forensics involves identifying malware, examining network intrusions, analyzing digital images and videos, and reviewing text and documents. The paper discusses the main challenges faced by researchers and practitioners, such as the need for quality training data, understanding ML models, and developing algorithms capable of keeping up with evolving digital threats. Furthermore, the review illustrates how ML has the potential to transform digital forensics by providing enhanced tools for detecting, organizing, and scrutinizing evidence, thereby helping to solve cybercrimes faster and more effectively.

The review by Aly et al. [38] analyzes research to uncover typical security challenges in IoT systems, including maintaining data confidentiality, verifying device identities, and ensuring network security. It also examines various strategies to enhance security, such as encryption, access control, and secure communication protocols. The paper emphasizes the necessity of a comprehensive security plan covering all aspects of internet-connected devices, from hardware to software. Additionally, the review highlights the need for ongoing research and innovation to keep pace with the evolving threats in the IoT field. The results of this study are highly relevant for stakeholders in the IoT industry, providing valuable insights for enhancing security and guiding future research in this area.

5.7. Legal and Ethical Considerations

The study by Dhaqm et al. [29] provides a thorough examination of the current status and potential development of various research domains in digital forensics. This includes investigations into personal computers, information systems, mobile devices, and cloud environments. The article presents the newest tools, techniques, and challenges in each field, emphasizing the importance of keeping pace with rapidly evolving technologies through continuous research and development. It also underscores the role of interdisciplinary collaboration and the integration of artificial intelligence and machine learning to advance forensic evidence collection. The study concludes by outlining primary areas for ongoing research and development in digital forensics to enhance its capabilities and readiness for the digital age.

The paper by Chetry et al. [21] offers a detailed scrutiny of the multiple methods and tools that memory forensic investigators can employ to extract valuable information from volatile memory. It highlights how memory analysis has become essential in uncovering and investigating serious online crimes, such as malware attacks, data breaches, and unauthorized access. The review discusses challenges in memory forensics, including the fragmented nature of trace data and the complexity of modern electronics. The authors stress the need for continuous improvement and adaptation of forensic tools and methods to address the ever-changing landscape of cybercrime. The paper concludes with insights into potential areas for research and development in memory forensics to further enhance its effectiveness against cyber threats.

Fernando et al. [12] present a broad discussion of cyber forensic tools and the challenges they encounter in keeping pace with the rapidly evolving digital environment. The paper explores various types of forensic tools used for investigating cybercrimes, including those for data acquisition, analysis, and reporting. It emphasizes the critical role of these tools in accurately collecting and analyzing digital evidence amidst the complex and error-prone nature of digital investigations. Furthermore, the article addresses contemporary challenges in cyber forensics, such as data encryption and cloud computing environments, which continue to advance in sophistication. It highlights the necessity for continual updates and enhancements to forensic tools to align with the evolving patterns of cybercrime. The study concludes by recommending future directions for research aimed at supporting the development of digital forensic tools capable of adapting to the changing demands of digital investigations.

The paper by Pallivalappil et al. [39] asserts that SSDs present unique challenges in digital forensics and incident response. It discusses the advantageous features of SSDs, such as wear leveling and garbage collection, and how these impact data retention and retrieval, posing challenges for forensic analysis. The paper examines procedures and tools designed to address data integrity issues specific to SSDs, illustrating the need to adapt traditional forensic methodologies to accommodate emerging SSD technologies. This underscores the implications of sophisticated computer-based offenses and the imperative to evolve forensic practices to effectively analyze SSDs.

The study by Likhar et al. [27] provides a comprehensive examination of memory forensics, with a specific focus on memory analysis techniques. It underscores the importance of analyzing volatile memory in digital investigations to uncover evidence that may not be recoverable from conventional storage media. The review elaborates on the tools and methodologies employed in memory forensics, including the extraction and analysis of data from RAM. It also addresses challenges associated with memory analysis, such as managing large volumes of data and the transient nature of digital information. The authors emphasize the crucial role that memory forensics plays in understanding the state of a system during an incident, making it an indispensable component of contemporary digital forensic investigations.

The study by Jones et al. [28] provides a comprehensive introduction to digital forensics, tracing its evolution from inception to its current state. It highlights significant milestones and advancements in the field, emphasizing various frameworks that guide forensic investigations, ensuring a systematic and methodical approach. The paper categorizes digital forensics into distinct domains, each presenting unique challenges and employing specialized techniques, such as computer, network, mobile, and cloud forensics. The review provides an overview of key tools utilized in digital forensic investigations, including equipment for data acquisition and processing, as well as specialized software tailored for specific forensic tasks. The article underscores the pivotal role of digital forensics in combating cybercrime and safeguarding cybersecurity in the digital era.

The study by Shree et al. [25] highlights the importance of capturing volatile memory data in a forensically sound manner, examining the complex process of acquiring data from multiple operating systems, including Windows, Linux, and macOS. Additionally, the paper discusses analysis techniques for extracting valuable information from memory dumps, such as identifying active processes, open network connections, and potentially malicious artifacts. The review sheds light on challenges and advancements in memory forensics, emphasizing its critical role in cybersecurity and digital investigations.

The study by Casino et al. [14] also emphasizes the significance of capturing volatile memory data in a forensically sound manner. It examines the complex process of acquiring data from multiple operating systems, including Windows, Linux, and macOS, and discusses methods for analyzing memory dumps to extract pertinent information, such as identifying active processes, open network connections, and potentially malicious artifacts. The review highlights ongoing challenges and developments in memory forensics, underscoring its crucial role in enhancing cybersecurity and supporting digital investigations.

6. Discussion

The landscape of cybercrime is constantly changing, presenting a significant opportunity to develop state-of-the-art analytical tools used in memory forensics. As criminals create more advanced methods, it is essential for memory forensic programs to evolve and keep up with these challenges [40]. This involves developing tools that excel in complex memory physiology analysis and detecting hidden malware signatures. Integrating AI and ML into memory forensics is an effective way to enhance the analysis process [12]. AI and ML algorithms can be trained to spot patterns and abnormalities in memory data, enabling automated detection of unusual activities. This automation can significantly ease memory forensic work, allowing analysts to focus on more sophisticated aspects of their investigations [41]. Another opportunity in memory forensics is the development of real-time memory-scanning solutions. These solutions can accelerate the detection and resolution of cyber threats by providing immediate insights into ongoing attacks, enabling rapid response and mitigation of threats [42]. Given the diversity of operating systems and hardware platforms, there is a need for a memory forensic toolset that is platform-independent. Providing integrative technology that can operate across various platforms will enhance the applicability of these tools in different forensic cases.

The effectiveness of memory forensics can be enhanced through intensified collaboration among researchers, practitioners, and stakeholders from various industries [29]. Communities can leverage this collaborative potential to accelerate the development of cutting-edge techniques and tools in forensics by sharing resources and knowledge [6]. This multi-party approach can also facilitate the creation of uniform rules and methods for memory investigation. By focusing on memory forensics, there is an opportunity to develop solutions that address the conflicting interests between information access and privacy principles [43]. This includes creating tools and techniques that limit the exposure of biographical information not directly related to forensic examinations. Finally, there is an opportunity to enhance memory forensics training and education for forensic analysts. As the field matures, lifelong learning becomes essential to support analysts with the latest advancements. This objective can be achieved through specialized training programs, workshops, and certifications designed to meet the needs of memory forensic professionals.

6.1. Challenges

A central problem and challenge in memory forensics is the volatile nature of memory. Data stored in volatile memory, such as RAM, are erased when the computer is turned off or shut down. The paper by Alghamdi et al. [42] highlights the inherent complexity and challenges of forensic analysis. Cybercriminals use encryption and obfuscation techniques to hide their activities and evade detection. Encrypted data in RAM are a significant problem for digital crime analysts, who must unlock the information using secret codes or more sophisticated techniques [14]. Another complexity is the use of obfuscation methods, such as code packing and polymorphism, which confuse experts by hiding malicious code and making it hard to detect and analyze. The vast amounts of data in modern large RAM can be overwhelming for forensic analysts [44]. Analyzing gigabytes or even terabytes of data is complicated and often overwhelming. This complexity is further compounded by the multilayered nature of memory, where different formats are accessible, requiring advanced tools and highly skilled technicians to handle the data.

The rapid pace of technological advancements poses another challenge for memory forensics, as hardware and software technologies continue to evolve, and criminals find and exploit new vulnerabilities. The ever-changing nature of evidence requires forensic techniques to be constantly developed, upgraded, and refined to effectively combat criminal activities [45]. Memory digital forensic analysis can be labor-intensive, requiring significant computational power and storage capacity for deep analysis of large datasets. Resource constraints can hamper the depth and breadth of forensic analysis, potentially affecting the quality and completeness of investigations [46]. Memory forensics operates within a legal and ethical framework that presents additional challenges. Privacy issues, data protection regulations, and the admissibility and veracity of evidence from memory forensics must be carefully managed to ensure that investigations are conducted legally and ethically. This sub-discipline of memory forensics demands a high level of expertise.

6.2. Limitations

One of the major limitations of this study is the relatively limited review of the available literature. This review does not include findings published earlier than the last ten years, and while this approach ensures the inclusion of the latest research findings, it may overlook valuable earlier works that formed the basis of current approaches in memory forensics. The possible drawback here is the exclusion of significant findings, potentially impacting the depth of information and knowledge obtained about the development of memory forensics. Additionally, the inclusion criteria for selecting papers may have created selection bias, leaving out studies of lower relevance or methodological quality. The reliance on randomized research, where negative and inconclusive studies might be missing from the analysis, could result in an overemphasis on predominantly positive outcomes, potentially overstating the actual efficacy of certain approaches or tools.

Another challenge that limits this line of work is methodological limitations. The review highly depends on the methodologies of the selected studies, which vary significantly in terms of rigor and reliability. Differences in sample sizes, experimental setups, and metrics used increase the possibility of contradictory results, making it challenging to provide concrete conclusions or conduct meta-analyses. Moreover, access to some studies and full-text articles was limited due to paywalls, potentially leading to the omission of valuable publications, especially those in less accessible databases. This limitation could result in a limited understanding of the current state of research in memory forensics, excluding works published in paywalled journals or books.

Another factor influencing the findings is the rapid pace of technological advancements in the field. Certain methodologies or tools described in the literature may already be outdated or replaced by more contemporary approaches, which could make recommendations vague or outdated. These limitations raise questions about the generalizability of the studied results, which are more suitable for observing the recent development history of memory forensics. The inconsistency in the quality of methodological approaches across different studies further complicates the delineation of clear results regarding various contexts or cases.

When applying the results and recommendations, proper care should be taken to understand these biases and limitations in scope. It is advised that the review be frequently updated to include current studies and new technologies to ensure that recommendations remain efficient and up-to-date. Future work should consider addressing these limitations by including older papers, using meta-analyses to manage methodological variability, and increasing the availability of various data types. To overcome these limitations and improve the state of memory forensics, interdisciplinary collaboration and improvements in research methodology will be essential.

6.3. Implications

6.3.1. Legal Frameworks and Regulations Impacting Memory Forensics

The GDPR in the European Union and CCPA in the United States are key regulations that help protect data rights and privacy. These regulations set stringent measures concerning the processing of personal data, including during forensic analysis. For example, under GDPR, personal data collected during memory forensics must be processed legally, transparently, and for specified purposes. Violations of these regulations are punishable by hefty fines and other legal consequences. Additionally, laws against cybercrimes in different jurisdictions define the legal framework within which digital investigations, including memory forensics, are conducted. These laws specify what is legal regarding the acquisition of electronic evidence, the extent of permissible investigation, and the handling of digital evidence in a manner that ensures its admissibility in court. Standards such as ISO/IEC 27037:2012 provide guidelines for the identification, collection, acquisition, and preservation of digital evidence, establishing procedural standards for forensic practice to ensure that investigations are systematic and reliable.

6.3.2. Ethical Issues in Memory Forensics

Ethical issues arise in any form of memory analysis, particularly concerning the reliability and integrity of the forensic process. Security is paramount because memory dumps can contain private details, ranging from passwords to secret keys and personal messages. Forensic analysts must handle these data ethically, focusing only on data relevant to the case and avoiding violations of individuals' privacy rights. Laws like GDPR and CCPA mandate that forensic experts implement measures to prevent data breaches and unauthorized access. Consent is another critical ethical concern; whenever possible, forensic examinations should be conducted with the permission of the individuals involved or, if permission cannot be obtained, through legal justification. It is also essential to ensure that sensitive information gathered during the forensic process is protected from alteration or misuse throughout the acquisition and analysis phases.

6.3.3. Role in Criminal Investigations

Memory forensics has become an essential tool in criminal investigations, especially in cybercrime cases. By investigating volatile memory, investigators can obtain valuable evidence such as active network traffic, running processes, and system states at the moment of malicious activity. This evidence is crucial for reconstructing events, identifying offenders, and understanding the motives behind the crime. The ability to retrieve such information provides law enforcement with fresh and vital data that are critical for securing convictions in criminal trials.

6.3.4. Impact on Privacy and Data Protection

The practice of memory forensics raises significant privacy and data protection issues due to the sensitive nature of the data involved. A memory dump can disclose confidential information such as personal data, passwords, encryption keys, and more. Extracting and analyzing this data requires utmost care to protect privacy and personal information [25].

Proper use of memory forensics within legal and ethical boundaries is essential to maintain public trust and uphold individual rights.

6.3.5. Legal and Regulatory Considerations

Memory forensics is subject to legal and regulatory scrutiny, which varies by jurisdiction [47]. Laws governing digital evidence, search and seizure, and data protection influence how memory forensic investigations are conducted. Failure to adhere to these legal norms can result in the inadmissibility of evidence in court and challenges to the forensic findings' validity. Therefore, forensic experts must have a comprehensive understanding of relevant legislation and regulations to navigate the legal landscape successfully.

6.3.6. Ethical Responsibilities

Memory forensic practitioners must adhere to ethical principles during investigations to ensure fairness, impartiality, and respect for data privacy. This includes obtaining proper authorization for forensic activities, minimizing unnecessary exposure of personal data, and maintaining the confidentiality and security of sensitive information [48]. Upholding ethical values is fundamental to ensuring that forensic processes are reliable while protecting the rights and dignity of those being investigated.

6.3.7. Implications for Policy and Governance

Memory forensics plays a vital role in cybersecurity and criminal investigations, significantly impacting policy and governance. Clearly defined policies and regulations are necessary to guide the use of memory forensic technology, including standards for evidence management, data protection, and ethical practices [16]. These policies should be developed collaboratively by government agencies, law enforcement, corporations, and academic institutions to strike a balance between security needs and the protection of privacy and civil rights.

6.4. Future Directions

Future studies in memory forensics should focus on creating standardized techniques and models to ensure correctness and uniformity in investigations. The development of automatic tools for real-time memory investigation could significantly modernize the cybersecurity field by enabling instant detection and reaction to cyber threats [49]. Additionally, research should concentrate on extending the scalability capacity of forensic tools to handle the volume of data in large-scale network systems and cloud environments. Analyzing existing legal and ethical issues, such as privacy violations and data protection, is crucial for advancing the field [10]. Furthermore, fostering interdisciplinary cooperation between computer science, law, psychiatry, and other disciplines can lead to novel approaches that consider the human factors in cybercrime and memory forensics [40]. Regular examination and improvement of the ethical and legal frameworks governing memory forensics are necessary as technology advances and security threats increase in number and complexity. This includes addressing questions related to why cybercrimes occur, how they can be prevented, and what types of memory-related evidence are admissible in legal trials. Table 2 outlines challenges in memory forensics along with mitigation strategies and future directions.

Table 2. Challenges, mitigations, and future directions in memory forensics.

Challenge	Mitigation	Future Direction
Volatility of memory	Develop rapid capture techniques and tools to preserve data quickly and accurately.	Advance real-time memory analysis capabilities to mitigate the impact of volatility.
Encryption and obfuscation	Implement specialized decryption techniques and tools to uncover hidden information.	Explore advanced analytical techniques to address encryption challenges, such as quantum computing.
Data volume and complexity	Utilize sophisticated tools and deep technical expertise to navigate and interpret complex memory structures.	Enhance the scalability of forensic tools to handle large-scale systems and cloud environments.
Rapid technological advancements	Continuously update and adapt forensic tools and methodologies to keep pace with new threats.	Foster interdisciplinary collaboration to innovate and develop adaptable forensic tools and methodologies.
Resource constraints	Optimize forensic tools for efficiency and develop scalable solutions for large memory dumps.	Invest in research to develop lightweight and efficient forensic tools.
Legal and ethical considerations	Ensure compliance with legal frameworks and ethical guidelines, and maintain integrity in investigations.	Continuously evaluate and update legal and ethical frameworks to align with technological advancements.
Skills gap	Enhance training and education programs for forensic professionals.	Promote interdisciplinary education to bridge the gap between technical expertise and legal knowledge.
Privacy and data protection concerns	Develop methodologies and tools that minimize the exposure of non-relevant personal data.	Advance privacy-preserving forensic techniques to balance investigation needs with privacy rights.

7. Future Recommendations

Future recommendations in memory forensics highlight the need for advanced malware detection techniques and improved memory analysis tools. Additionally, research should focus on addressing challenges posed by cloud computing, integrating AI, and ensuring methodological standards for reliable investigations while embracing emerging trends like edge computing and IoT.

7.1. Areas for Further Research

In the ever-changing landscape of memory forensics, there are numerous areas ripe for further exploration. A key area of focus is the development of advanced techniques to detect sophisticated malware. Modern malware often employs anti-forensic measures designed to hide its presence in memory, making it a challenge for forensic investigators to identify and analyze. By creating more refined detection methods, researchers can help stay one step ahead of these evolving threats.

Another critical area for research is the enhancement of memory analysis tools. As the complexity and size of memory dumps continue to grow, there is a pressing need for tools that can handle these data more efficiently and accurately. Improvements in this area could significantly speed up the forensic analysis process and provide more reliable results.

Cloud computing has become a dominant force in the technology landscape, bringing with it new challenges for memory forensics. As more organizations move their operations to the cloud, the need for effective memory forensic techniques in these environments becomes increasingly important. Research is needed to develop methods for remote memory acquisition and analysis that can work effectively in the multi-tenant environments typical of cloud computing. This includes finding ways to securely and efficiently access and analyze memory data from virtual machines and other cloud-based resources.

Overall, the field of memory forensics is at a critical juncture, with numerous opportunities for research that can advance our capabilities in detecting and analyzing digital threats in an increasingly complex technological world.

7.2. Emerging Trends and Technologies

In the dynamic field of memory forensics, several emerging trends and technologies are shaping the future of investigations. One of the most significant developments is the integration of machine learning and artificial intelligence into forensic tools. These technologies have the potential to revolutionize memory forensics by automating the detection of anomalies and malicious patterns, significantly reducing the time and effort required for analysis.

Another trend gaining traction is the use of hardware-assisted virtualization technologies. These technologies offer a secure and efficient way to isolate and analyze memory, providing a layer of protection against tampering and ensuring the integrity of forensic data. This is particularly important in environments where the security of forensic processes is paramount.

The integration of memory forensics with other digital forensic disciplines, such as network and disk forensics, is becoming increasingly crucial. As cyber incidents become more complex, a holistic approach to investigations is necessary to uncover the full scope of an incident. By combining insights from different forensic domains, investigators can construct a more comprehensive picture of the events that occurred.

The advent of new computing paradigms, such as edge computing and the Internet of Things, presents both challenges and opportunities for memory forensics research. These technologies introduce new types of devices and data sources that forensic investigators need to consider. As a result, there is a growing need for research into methods and tools that can effectively handle the unique characteristics of memory data in these environments.

Overall, these emerging trends and technologies are pushing the boundaries of what is possible in memory forensics, offering exciting possibilities for advancing the field and enhancing our ability to respond to cyber threats.

7.3. Methodological Improvements

To bolster the reliability and effectiveness of memory forensics investigations, several methodological improvements are necessary. Firstly, developing standardized procedures for memory acquisition and analysis is paramount. Standardization ensures that investigations are conducted consistently across different cases, enhancing the reliability of the findings. This includes establishing clear guidelines for capturing memory data, analyzing them, and documenting the process.

Secondly, there is a pressing need for more robust validation and testing frameworks for memory forensic tools. As the tools used in memory forensics play a crucial role in the investigation process, their accuracy and reliability are of utmost importance. A comprehensive validation and testing framework can help identify any weaknesses or inaccuracies in these tools, ensuring that they provide reliable results.

Enhancing the integration of memory forensics with other forensic tools and workflows is crucial for improving the overall efficiency of investigations. By creating seamless connections between memory forensic tools and other digital forensic tools, investigators can streamline their workflows and reduce the time needed to piece together evidence from different sources.

8. Conclusions

The systematic literature review on memory forensics within cybersecurity is a rigorous review, emphasizing the essential elements of the field throughout digital investigations. This article uses a strict selection process, which involves scrutinizing existing research papers on forensic methods, the effects of technological advancements, and key ethical and legal challenges. It ensures the acceptance of the most relevant and authoritative studies through a preliminary review, in-depth full-text evaluation, and consensus conference. This approach not only ensures high-quality literature but also identifies areas for improvement and potential research opportunities.

The SLR highlights the dynamic nature of cybercrime, which requires highly advanced, flexible, and modern forensic tools and techniques for investigations. The integration of recent technologies like AI and ML in memory forensics is highlighted as a promising step, potentially revolutionizing the field by enabling the detection and analysis of threats and raising the possibility of real-time memory scanning for immediate threat response. The significance of platform-independent forensic tools is emphasized, given the diversity of systems and hardware. Furthermore, there is a need for collaboration among different stakeholders and the standardization of tools.

While the unpredictable and volatile nature of memory data, complex encryption and obfuscation methods used by cybercriminals, and the large volume and complexity of memory data are considered significant challenges, the development of sophisticated detection techniques, advancement of memory analysis tools, and constant methodological adaptation are necessary. Legal and ethical issues, particularly concerning privacy, data protection, and the admissibility of evidence in legal proceedings, are also crucial.

Future research directions in memory forensics should focus on developing standardized models and techniques for reliability and accuracy, creating automatic tools for real-time analysis, increasing the scalability of forensic tools for large-scale systems and cloud environments, and addressing legal and ethical issues related to data protection and privacy. Interdisciplinary cooperation is encouraged to enable comprehensive research that accounts for human factors in cybercrime and memory forensics.

Author Contributions: Conceptualization, I.H. and M.M.H.R.; methodology, I.H. and M.M.H.R.; validation, I.H. and M.M.H.R.; formal analysis, I.H. and M.M.H.R.; investigation, I.H. and M.M.H.R.; resources, I.H. and M.M.H.R.; writing—original draft preparation, I.H. and M.M.H.R.; writing—review and editing, I.H. and M.M.H.R.; visualization, I.H. and M.M.H.R.; supervision, M.M.H.R.; funding acquisition, I.H. and M.M.H.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. 241306].

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data was created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. 241306]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which improved the quality and clarity of the paper.

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

References

1. Strandberg, K.; Nowdehi, N.; Olovsson, T. A systematic literature review on automotive digital forensics: Challenges, technical solutions and data collection. *IEEE Trans. Intell. Veh.* **2022**, *8*, 1350–1367. [CrossRef]
2. Coronel, B.; Cedillo, P.; Campos, K.; Camacho, J.; Bermeo, A. A systematic review in cyber forensics: Current trends from the client perspective. In Proceedings of the 2018 IEEE Third Ecuador Technical Chapters Meeting (ETCM), Cuenca, Ecuador, 15–19 October 2018; pp. 1–6.
3. Ishrag Hamid, R.A.; Riad, K. Advancing Malware Artifact Detection and Analysis through Memory Forensics: A Comprehensive Literature Review. *J. Theor. Appl. Inf. Technol.* **2024**, *102*, 1–16.
4. Maneli, M.A.; Isafiade, O.E. 3D forensic crime scene reconstruction involving immersive technology: A systematic literature review. *IEEE Access* **2022**, *10*, 88821–88857. [CrossRef]
5. Hamid, I.; Alabdulhay, A.; Hafizur, Rahman, M.M. A systematic literature review on volatility memory forensics. In *Computational Vision and Bio-Inspired Computing*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 589–600.

6. Manral, B.; Somani, G.; Choo, K.K.R.; Conti, M.; Gaur, M.S. A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–38. [CrossRef]
7. Bai, V.S.; Sudha, T. A systematic literature review on cloud forensics in cloud environment. *Int. J. Intell. Syst. Appl. Eng.* **2023**, *11*, 565–578.
8. Bahrum, N.N.; Setumin, S.; Abdullah, M.F.; Maruzuki, M.I.F.; Che Ani, A.I. A systematic review of face sketch recognition system. *J. Electr. Electron. Syst. Res.* **2023**, *22*, 1–10. [CrossRef]
9. Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Abd Razak, S.; Grispos, G.; Choo, K.K.R.; Al-Rimy, B.A.S.; Alsewari, A.A. Digital forensics subdomains: The state of the art and future directions. *IEEE Access* **2021**, *9*, 152476–152502.
10. Al-Dhaqm, A.; Abd, Razak, S.; Othman, S.H.; Ali, A.; Ghaleb, F.A.; Rosman, A.S.; Marni, N. Database forensic investigation process models: A review. *IEEE Access* **2020**, *8*, 48477–48490.
11. Lutta, P.; Sedky, M.; Hassan, M.; Jayawickrama, U.; Bastaki, B.B. The complexity of internet of things forensics: A state-of-the-art review. *Forensic Sci. Int. Digit. Investig.* **2021**, *38*, 301210. [CrossRef]
12. Fernando, V. Cyber forensics tools: A review on mechanism and emerging challenges. In Proceedings of the 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 19–21 April 2021; pp. 1–7.
13. Ghosh, A.; Majumder, K.; De, D. A systematic review of digital, cloud and iot forensics. In *The "Essence" of Network Security: An End-to-End Panorama*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 31–74.
14. Casino, F.; Dasaklis, T.K.; Spathoulas, G.P.; Anagnostopoulos, M.; Ghosal, A.; Borocz, I.; Solanas, A.; Conti, M.; Patsakis, C. Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access* **2022**, *10*, 25464–25493. [CrossRef]
15. Paul Joseph, D.; Norman, J. A review and analysis of ransomware using memory forensics and its tools. In *Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics*; Springer: Singapore, 2020; Volume 1, pp. 505–514.
16. Gancedo, Y.; Fariña, F.; Seijo, D.; Vilariño, M.; Arce, R. Reality monitoring: A meta-analytical review for forensic practice. *Eur. J. Psychol. Appl. Leg. Context* **2021**, *13*, 99–110. [CrossRef]
17. Chopade, R.; Pachghare, V.K. Ten years of critical review on database forensics research. *Digit. Investig.* **2019**, *29*, 180–197. [CrossRef]
18. Taylor, J.; Turnbull, B.; Creech, G. Volatile memory forensics acquisition efficacy: A comparative study towards analysing firmware-based rootkits. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 1–11.
19. Nyholm, H.; Monteith, K.; Lyles, S.; Gallegos, M.; DeSantis, M.; Donaldson, J.; Taylor, C. The evolution of volatile memory forensics. *J. Cybersecur. Priv.* **2022**, *2*, 556–572. [CrossRef]
20. Osbourne, G. Memory forensics: Review of acquisition and analysis techniques. *Defence Sci. Technol. Organ. Edinb. Cyber Electron. Warfare Div, Tech. Rep.* **2013**.
21. Chetry, A.; Sharma, U. Memory forensics analysis for investigation of online crime-a review. In Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 13–15 March 2019; pp. 40–45.
22. Pagani, F.; Fedorov, O.; Balzarotti, D. Introducing the temporal dimension to memory forensics. *ACM Trans. Priv. Secur. (TOPS)* **2019**, *22*, 1–21.
23. Daghmehchi Firoozjaei, M.; Habibi Lashkari, A.; Ghorbani, A.A. Memory forensics tools: A comparative analysis. *J. Cyber Secur. Technol.* **2022**, *6*, 149–173. [CrossRef]
24. Latzo, T.; Palutke, R.; Freiling, F. A universal taxonomy and survey of forensic memory acquisition techniques. *Digit. Investig.* **2019**, *28*, 56–69. [CrossRef]
25. Shree, R.; Shukla, A.K.; Pandey, R.P.; Shukla, V.; Bajpai, D. Memory forensic: Acquisition and analysis mechanism for operating systems. *Mater. Today Proc.* **2022**, *51*, 254–260. [CrossRef]
26. Ostrovskaya, S.; Skulkin, O. *Practical Memory Forensics: Jumpstart Effective Forensic Analysis of Volatile Memory*; Packt Publishing Ltd.: Birmingham, UK, 2022.
27. Likhar, D.; Rajput, M. Study of Memory Forensics: Memory Analysis Technique. *Memory* **2019**, *7*, 2333–2335.
28. Jones, G.M.; Winster, S.G. An insight into digital forensics: History, frameworks, types and tools. In *Cyber Security and Digital Forensics*; Wiley: Hoboken, NJ, USA, 2022; pp. 105–125.
29. Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Razak, S.; Ghabban, F.M. Research challenges and opportunities in drone forensics models. *Electronics* **2021**, *10*, 1519. [CrossRef]
30. Alharbi, S.; Weber-Jahnke, J.; Traore, I. The proactive and reactive digital forensics investigation process: A systematic literature review. In Proceedings of the Information Security and Assurance: International Conference, ISA 2011, Brno, Czech Republic, 15–17 August 2011; pp. 87–100.
31. Pandey, A.K.; Tripathi, A.K.; Kapil, G.; Singh, V.; Khan, M.W.; Agrawal, A.; Kumar, R.; Khan, R.A. Current challenges of digital forensics in cyber security. In *Critical Concepts, Standards, and Techniques in Cyber Forensics*; IGI Global: Pennsylvania, PA, USA, 2020; pp. 31–46.
32. Al-Dhaqm, A.; Abd Razak, S.; Ikuesan, R.A.; Kebande, V.R.; Siddique, K.A review of mobile forensic investigation process models. *IEEE Access* **2020**, *8*, 173359–173375. [CrossRef]

33. Azzery, Y.; Mulyanto, N.D.; Hidayat, T. Memory Forensic Development and Challenges in Identifying Digital Crime: A Review. *Teknokom* **2022**, *5*, 96–102. [CrossRef]
34. Ganesh, N.G.; Venkatesh, N.M.; Prasad, D.V.V. A systematic literature review on forensics in cloud, IoT, AI & blockchain. In *Illumination of Artificial Intelligence in Cybersecurity and Forensics*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 197–229.
35. Sjöstrand, M. Combatting the Data Volume Issue in Digital Forensics: A Structured Literature Review. Independent Thesis, School of Informatics, University of Skövde, Skövde, Sweden, 2020. Available online: https://www.essays.se/essay/6451f12a1d/ (accessed on 23 June 2024).
36. Case, A.; Maggio, R.D.; Firoz-Ul-Amin, M.; Jalalzai, M.M.; Ali-Gombe, A.; Sun, M.; Richard, G.G., III. Hooktracer: Automatic detection and analysis of keystroke loggers using memory forensics. *Comput. Secur.* **2020**, *96*, 101872. [CrossRef]
37. Nayerifard, T.; Amintoosi, H.; Bafghi, A.G.; Dehghantanha, A. Machine learning in digital forensics: A systematic literature review. *arXiv* **2023**, arXiv:2306.04965.
38. Aly, M.; Khomh, F.; Haoues, M.; Quintero, A.; Yacout, S. Enforcing security in Internet of Things frameworks: A systematic literature review. *Internet Things* **2019**, *6*, 100050. [CrossRef]
39. Pallivalappil, A.S.; Jagadeesha, S.N. Procedures for Digital Forensics and Incident Response on Including Data Integrity Constraints on Solid-State Drives (SSD)-A Literature Review. *Int. J. Case Stud. Bus. IT Educ. (IJCSBE)* **2022**, *6*, 328–350. [CrossRef]
40. Montasari, R.; Hill, R. Next-generation digital forensics: Challenges and future paradigms. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019; pp. 205–212.
41. Dawson, L.; Akinbi, A. Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study. *Forensic Sci. Int. Rep.* **2021**, *3*, 100198. [CrossRef]
42. Alghamdi, M.I. Digital forensics in cyber security—Recent trends, threats, and opportunities. In *Cybersecurity Threats with New Perspectives*; Books on Demand: Norderstedt, Germany, 2021.
43. Servida, F.; Casey, E. IoT forensic challenges and opportunities for digital traces. *Digit. Investig.* **2019**, *28*, S22–S29. [CrossRef]
44. Tiwari, A.; Mehrotra, V.; Goel, S.; Naman, K.; Maurya, S.; Agarwal, R. Developing trends and challenges of digital forensics. In Proceedings of the 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 22–23 October 2021.
45. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations. *arXiv* **2021**, arXiv:2103.17028.
46. Zhang, N.; Zhang, R.; Sun, K.; Lou, W.; Hou, Y.T.; Jajodia, S. Memory forensic challenges under misused architectural features. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2345–2358. [CrossRef]
47. Javeed, D.; Khan, M.T.; Ahmad, I.; Iqbal, T.; Badamasi, U.M.; Ndubuisi, C.O.; Umar, A. An efficient approach of threat hunting using memory forensics. *Int. J. Comput. Netw. Commun. Secur.* **2020**, *8*, 37–45. [CrossRef] [PubMed]
48. Thomas, T.; Piscitelli, M.; Nahar, B.A.; Baggili, I. Duck Hunt: Memory forensics of USB attack platforms. *Forensic Sci. Int. Digit. Investig.* **2021**, *37*, 301190. [CrossRef]
49. Qawasmeh, E.; Al-Saleh, M.I.; Al-Sharif, Z.A. November. Towards a generic approach for memory forensics. In Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 20–21 November 2019; pp. 094–098.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.