Research Trends, Challenges, and Emerging Topics in Digital Forensics

A Review of Reviews

Casino, Fran; Dasaklis, Thomas K.; Spathoulas, Georgios P.; Anagnostopoulos, Marios; Ghosal, Amrita; Borocz, Istvan; Solanas, Agusti; Conti, Mauro; Patsakis, Constantinos

Published in:
IEEE Access

DOI (link to publication from Publisher):
10.1109/ACCESS.2022.3154059

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 22, 2022, accepted February 16, 2022, date of publication February 24, 2022, date of current version March 10, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3154059

Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews

FRAN CASINO[1,2], (Member, IEEE), THOMAS K. DASAKLIS[3], GEORGIOS P. SPATHOULAS[4], MARIOS ANAGNOSTOPOULOS[5], AMRITA GHOSAL[6], ISTVÁN BOŐOCZ[7], AGUSTI SOLANAS[1], (Senior Member, IEEE), MAURO CONTI[8,9], (Fellow, IEEE), AND CONSTANTINOS PATSAKIS[2,10]

[1]Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, 43007 Tarragona, Spain
[2]Information Management Systems Institute, Athena Research Center, 151 25 Marousi, Greece
[3]Hellenic Open University, 570 01 Patras, Greece
[4]Norwegian University of Science and Technology (NTNU), 2802 Gjøvik, Norway
[5]Aalborg University, 9220 Copenhagen, Denmark
[6]CONFIRM Centre, University of Limerick, Limerick, V94 T9PX Ireland
[7]Vrije Universiteit Brussel, 1050 Brussels, Belgium
[8]Department of Mathematics, University of Padua, 35122 Padua, Italy
[9]Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, 2628 CD Delft, The Netherlands
[10]Department of Informatics, University of Piraeus, 185 34 Piraeus, Greece

Corresponding author: Constantinos Patsakis (kpatsak@unipi.gr)

This work was supported in part by the European Commission under the Horizon 2020 Programme (H2020), as part of the projects LOCARD under Grant 832735, HEROES under Grant 101021801, and the CyberSec4Europe under Grant 830929; and in part by the European Commission (call ISFP-2020-AG-TERFIN) as part of the CTC Project under Grant 830929. The work of Fran Casino was supported by the Beatriu de Pinós programme of the Government of Catalonia under Grant 2020 BP 00035.

ABSTRACT Due to its critical role in cybersecurity, digital forensics has received significant attention from researchers and practitioners alike. The ever increasing sophistication of modern cyberattacks is directly related to the complexity of evidence acquisition, which often requires the use of several technologies. To date, researchers have presented many surveys and reviews on the field. However, such articles focused on the advances of each particular domain of digital forensics individually. Therefore, while each of these surveys facilitates researchers and practitioners to keep up with the latest advances in a particular domain of digital forensics, the global perspective is missing. Aiming to fill this gap, we performed a qualitative review of all the relevant reviews in the field of digital forensics, determined the main topics on digital forensics topics and identified their main challenges. Despite the diversity of topics and methods, there are several common problems that are faced by almost all of them, with most of them residing in evidence acquisition and pre-processing due to counter analysis methods and difficulties of collecting data from devices, the cloud etc. Beyond pure technical issues, our study highlights procedural issues in terms of readiness, reporting and presentation, as well as ethics, highlighting the European perspective which is traditionally stricter in terms of privacy. Our extensive analysis paves the way for closer collaboration among researcher and practitioners among different topics of digital forensics.

INDEX TERMS Digital forensics, cybersecurity, review of reviews, forensic investigations, meta review.

I. INTRODUCTION

According to Edmond Locard's exchange principle, in every crime, the perpetrator will alter the crime scene by bringing something and leaving something else [1], [2]. Therefore, these changes can be used as forensic evidence. While this principle is relatively straightforward, it is difficult in many cases to apply. This is why Locard introduced forensics labs in Law Enforcement Agencies (LEAs) over the first decade of the 20th century [3].

While procedures that resemble digital forensics are mentioned in computer science literature quite early, the domain was not fully defined until 1980s when it started to gain attention. The introduction of the IBM PC generalised the

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

use of computing machines; thus, more interest was focused on digital evidence and many people came together and created a digital forensics community, which eventually became more formal in 1993 when the FBI hosted the First International Conference on Computer Evidence [4]. Initially, the main activity was examining standalone computers to recover deleted or destroyed files from the disks. However, since the early 2000s, the digital forensics domain has expanded steadily, maturing along with regulations [5], [6]. Nowadays, users tend to utilise multiple digital devices and access tenths of digital services per day [7], [8]. The digital footprint of our everyday life has become enormous, and accordingly the probability that illegal activities leave digital evidence behind is very high. The need for forensic investigators has increased, and this have led to multiple academic education and certification programs related to digital forensics [9]. Additionally, the complexity of the tasks to be carried out and the required compliance with law and courts' regulations has led to the establishment of strict protocols and procedures to be followed [10]–[12]. The continuous appearance of new forms of cybercrime also requires adaptive investigation process models, new technology, and advanced techniques to deal with such incidents [13]–[15].

Beyond the rise of cybercrime, where the evidence is expected to be digital, digital evidence is underpinning almost all modern crime scenes. For instance, mobile devices have become a primary source of digital evidence as almost all our communications are performed through them [6]. In fact, according to EU,[1] the bulk of criminal investigations (85%) involve electronic evidence. Thus, emails, cloud service providers, online payments, and wearable devices are often used to extract digital evidence in various circumstances.

A. MOTIVATION

Digital evidence has become a norm and underpins most modern crime investigations. However, there are digital evidence to which different methods and methodologies apply. Some principles may remain the same; however, they cannot be applied to all types of evidence. For instance, collecting evidence from the Cloud bears no resemblance to IoT forensics or image forensics. This has led to a huge amount of research, which addresses the challenges raised in each domain individually, with the bulk of the work devoted to the development of novel tools and algorithms to extract digital evidence and intelligence from heterogeneous sources. Currently, investigators devote many efforts to provide a systematic overview of the literature and the advances in each domain, with focused surveys and reviews. Despite the importance of these surveys, an analysis considering the challenges and issues of the different digital forensics domains as a whole is still missing. In other words, each of these surveys is focused on a specific domain and, as a result, common issues, challenges and methods are not identified. Moreover, research directions and approaches, that could be applied in several domains, remain explored in a topic-wise manner, lacking interoperability, and denoting a lack of collaboration between researchers in different forensics domains. We sustain that the above is a serious gap in current literature, and we aim to fill it in this article. To this end, we present a review of reviews in the field of digital forensics.

[1] https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

B. CONTRIBUTION

According to a thorough methodological research, we collect all relevant surveys and reviews in the field of digital forensics, analyse them, and answer a set of research questions, listed in Table 1, by performing the following actions:

- Analysing the current state of the art and practice, and identifying the challenges of each domain individually.
- Assessing whether the current state of the art is aligned with the technological evolution in digital forensics.
- Using the previously collected information to identify common issues, gaps, best strategies and key focus areas in digital forensics, trying to span across different domains.
- Assessing technological advances to highlight emerging challenges in digital forensics.

In addition to suggesting promising research lines in the field based on the above analysis, we cover other dimensions of digital forensics, including frameworks and process models, standardisation, readability and reporting, as well as legal and ethical aspects. To the best of our knowledge, this is the first review of reviews covering the state of the art in digital forensics and showcasing the actual state of practice from a global perspective.

The remainder of the article is organized as follows: Section II details our research methodology, providing a descriptive analysis of the retrieved literature, which is then complemented with a taxonomy of digital forensics in Section III. Section IV analyses the current state of practice regarding forensic methodologies and their phases, standards, and ethics. Relevant open issues, trends, and further research lines are discussed in Section V. The article concludes in Section VI with some final remarks.

II. RESEARCH METHODOLOGY

In recent years, academic publishing has significantly increased both in terms of volume and speed. At the same time, new channels for publication, such as conference proceedings, open archives and numerous scientific journals, are rapidly expanding, thus allowing today's researchers to publish their work in a multitude of venues [16]. According to recent studies, approximately 22 new systematic reviews are published daily [17]. New methodological approaches for synthesising this evidence have been developed to keep up with the proliferation of systematic reviews across disciplines. Besides, conducting reviews of existing systematic reviews has become a logical next step in providing evidence in domains where a growing number of systematic reviews is available. Overviews or umbrella reviews are most commonly

TABLE 1. Summary of research questions and the corresponding sections devoted to answer them.

Research Question	Objective	Relevant Sections
What is the current state of practice and research trends in digital forensics?	To address this question, we will analyse the digital forensics literature to identify the research trends and the topics that require more support. Furthermore, such analysis will streamline common solutions and practices that can be fostered by other domains.	2, 3 and 4
Which are the current challenges in digital forensics?	To answer this question, our strategy is to extract the digital forensics challenges from local and global perspectives to provide a comprehensive overview of such a multidisciplinary field. This will highlight each digital forensics domain's particularities and stress their commonalities.	3 and 4
Is the current state of the art aligned with technological evolution in digital forensics?	The objective of this question is to discover whether the actual state of the art, in terms of e.g., technologies, legislation and standards, is sufficient to cope with modern cybercrime. This can serve as a road map for tool development, prioritisation standardisation actions, etc.	3, 4 and 5
What strategies should be used to deal with identified challenges?	This question aims to identify the pain points of the actual state of practice and leverage a gap analysis to provide fruitful strategies.	4 and 5
Based on technological advances and trends, what challenges will digital forensics face in the future?	The goal of this question is to identify characteristics and critical issues in emerging technologies that may hinder digital investigations in the near future. Timely identifying these issues and prioritising R&D actions will significantly decrease their potential impact.	5

used to bring together, appraise, and synthesise the results of related systematic reviews when multiple systematic reviews on similar or related topics already exist [17], [18]. Therefore, a review of reviews or an umbrella review compiles evidence from multiple reviews or survey papers into a single document. Syntheses of previous systematic reviews are known by a variety of names, one of which is an umbrella review. Other descriptions include the terms (''review of reviews,'' ''systematic review of reviews,'' ''review of systematic reviews,'' ''overviews of reviews,'' ''summary of systematic reviews,'' ''summary of reviews,'' and ''synthesis of reviews'') [19].

Despite their growing popularity, no standardized reporting guidelines currently exist for umbrella reviews. However, various multidisciplinary teams around the globe work together to develop relevant standardized reporting guidelines that will soon be available [20]. In our case, we rely upon an entirely systematic way to conduct our umbrella review. In particular, we have used various features of the approach presented in [21] to conduct our review of reviews and provide a transparent, reproducible and sound overview of the scientific literature on digital forensics from a global perspective. Our review protocol consists of five steps, as shown in Figure 1: 1) Planning the review 2) Defining research questions 3) Searching literature databases 4) Applying inclusion and exclusion criteria and 5) Synthesising and reporting the results of the literature analysis.

FIGURE 1. Detail of the research methodology steps.

A. SEARCH STRATEGY

As previously stated, our overall survey process is based on several predefined research questions relevant to the digital forensics literature. We conducted extensive research addressing the various technical/functional/security challenges of the digital forensics literature guided by these research questions. To this end, we performed a systematic literature search without time constraints in May 2021 which was subsequently updated in November 2021. The main search engines used were Web of Science (WoS), Scopus and Google. Scopus and WoS were used to locate all scientific-related literature due to their multidisciplinary coverage and scope [22], while Google was used to locate relevant standards and best practices (grey literature). We queried Scopus and WoS using the terms ''*digital forensics and review or survey*'' in the title, keywords, and abstract of all articles. It is worth noting that first bulk search query yielded 536 unique results (combining both sources).

Electronic searches using Google also turned up relevant *grey literature*, such as unpublished research commissioned by governments or private/public institutions. In particular, we looked at the first 200 Google results for the queries *digital forensics and reviews* and *digital forensics and surveys* to find the published grey literature. It is worth noting that we used Google searches as a supplement to our primary search strategy (especially for streamlining the assessment), and Scopus and WoS were our primary source for finding scientific-related literature. Furthermore, compared to the bibliography retrieved from Scopus and WoS, the total number of documents retrieved from Google was relatively low.

We discovered additional studies using the so-called snowball effect (backward and forward), which involved searching the references of key articles and reports for additional citations [23]. For instance, additional grey literature was discovered by manually searching the reference lists in several reports, particularly research and committee reports or policy briefs from private and public sector institutions/organizations. For this study, we take into consideration 109 research papers and 51 reports. The 109 papers are used for identifying relevant challenges/trends across different digital forensics domains (see Section III). The 51 reports were used to derive further insights about the state of practice regarding digital forensics methodologies, practices and standards, as well as discussing future trends and open challenges from a policy perspective (see sections IV and V).

B. SELECTION OF STUDIES

We used various pre-defined exclusion and inclusion criteria as described in Table 2 to assess the eligibility of the retrieved literature; both academic and grey. Some exclusion criteria were used before introducing the literature into the bibliographic manager (language, subject area and document type restrictions). It is also worth noting that we have only examined review papers and reports written in English.

Our overall selection process steps are the following: (i) We initially evaluated the relevance of the titles of all scientific articles and reports. Articles/reports fulfilling one of the exclusion criteria were removed from the analysis and sorted according to the reason for their removal, (ii) In the sequence, we evaluated the relevance of all paper abstracts and report introduction sections (grey literature). Articles and/or reports that met one of the defined exclusion criteria were excluded from the analysis, and we documented the reason for exclusion, (iii) We also did a full-text reading, and some additional articles/reports were excluded and sorted by reason of exclusion during this step. We resolved any potential disagreements among authors about the relevance of the retrieved articles/reports through discussion until reaching a unanimous consensus. We omitted several studies because they were not reviews or surveys (for example, papers relevant to financial forensics investigation, business forensics). We also discarded from the analysis articles that did not meet the inclusion criteria.

C. ANALYSIS AND REPORTING

All articles and/or reports that met the inclusion criteria were analyzed (in emerging themes) using a qualitative analysis software (MAXQDA11). The authors carried out the thematic content analysis independently. We applied various qualitative analysis methods (such as narrative synthesis and thematic analysis) to classify and synthesise the extracted data in a sound and comprehensive manner. The results of our analysis are presented in sections III and IV.

D. BIBLIOGRAPHIC ANALYSIS

In this section, we present a descriptive analysis of the scientific papers included in the challenges-based and domain-specific classification (see Figure 2). The descriptive analysis includes 109 research papers published from 2006 until the end of November 2021. The purpose of the descriptive analysis presented is three-fold:

1) It enhances the statistical description, aggregation, and presentation of the constructs of interest or their associations of the relevant literature (publications per year and domain etc.).
2) It contains insights to current research trends in the area of digital forensics and a critical discussion of the challenges identified. It, therefore, supports the classification structure presented in Section III
3) It allows us to visually demonstrate the diverse research approaches used up to this point in the scientific literature regarding the proliferation of digital forensics review papers.

The distribution of publications over time is depicted in Figure 2. In particular, Figure 2 shows a year-by-year analysis of the selected papers. It is worth noting that the number of publications has increased significantly after 2017. Until the end of 2017, there were only about 38 review papers addressing issues of digital forensics. However, from 2017 onwards, the number of reviews published in the scientific literature has risen to nearly 70. As a result, over the last four years, research in the area of digital forensics has slowly but steadily increased. This upward trend reflects the key public and policy impact of digital forensics nowadays.

Figure 2 also shows the domain-specific distribution of the 109 review papers included in our analysis. It is worth noting that we have identified seven (7) prevalent areas of research interest in digital forensics: Blockchain, Cloud, Filesystem and databases, Multimedia, IoT, Mobile, Networks. Multimedia forensics attracts most of the current digital forensics research (38 out of the 109 review papers), followed by Filesystem and database forensics papers (18 out of 109). Both streams justify that the widespread use of mobile devices with lower-cost storage and increased bandwidth has resulted in a massive generation of multimedia-related content. Furthermore, various miscellaneous review papers (applications that do not fit into any of the above categories) demonstrate the digital forensics multidisciplinary nature. These multidisciplinary review papers

TABLE 2. Selection criteria of the retrieved literature.

Selection criteria	Scientific database		Grey literature
Inclusion	Only peer-reviewed scientific research papers (including articles in press, written in English)		Industry reports, committee reports, policy briefs (written in English)
	Without time-frame restrictions		Without time-frame restrictions
Exclusion	Before import to the bibliographic manager	Non English-written papers, papers published in conference proceedings, book chapters, papers with missing abstracts etc.	Generic reports relevant to digital forensics without describing standardized processes of digital forensics investigation.
	During abstract screening	Papers belonging to other discipline than digital forensics	
	During full-text reading	Papers describing forensics process models, and/or papers not identifying or discussing challenges	

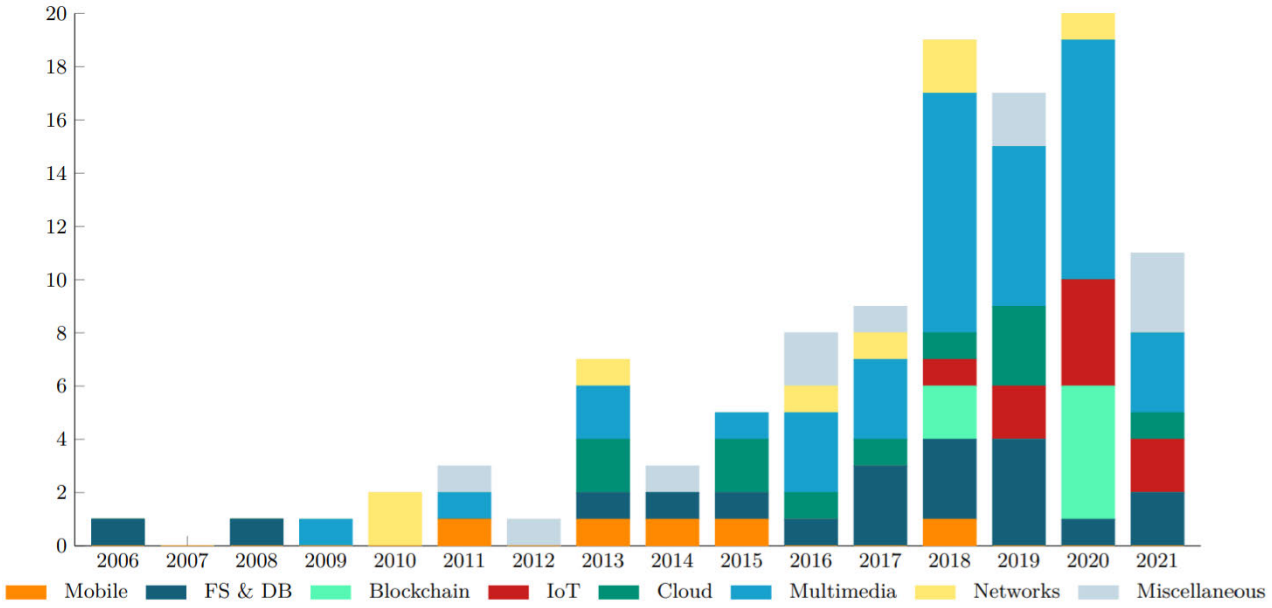

FIGURE 2. Year-wise analysis of the selected literature per domain.

represent research conducted in areas such as social media, smart grid, unmanned aerial vehicles and etc.

III. TAXONOMY OF CHALLENGES-BASED DIGITAL FORENSICS RESEARCH

In this section, we summarise the surveys/literature reviews collected following a rigorous statistical methodology based on the literature, as described in Section II. The topics of this classification have been systematically selected according to the contents of reviewed literature, and thus reflect the digital forensics research landscape and illustrates with high fidelity the heterogeneity of digital forensic solutions. The classification of digital forensics topics is graphically represented in Figure 3. In each case, we discuss the main limitations and challenges proposed in the literature. More precisely, we extract the challenges at a research field domain level (i.e., we group in a higher hierarchical level, when possible, the limitations of the methods presented in the surveys) to give a more comprehensive perspective and to enable further cross-topic comparisons in Section III-I.

A. CLOUD

Researchers, as well as government agencies, have thoroughly explored many of the challenges in cloud forensics, though some challenges still remain to be addressed. For example, the diversity of embedded OSs with shorter product life cycles, as well as the numerous smartphone manufacturers around the world present, are challenges in this research area. In the literature, we can find research works that have addressed challenges in cloud forensics and their solutions from different perspectives. Purnaye *et al.* [7] explored the different dimensions of cloud fornesics and categorised the main challenges of this topic. Alex *et al.* [24] discussed challenges in cloud forensics related to data acquisition, logging, dependence on cloud service providers, chain of custody, crime scene reconstruction, cross border law and law presentation. Khanafseh *et al.* [25] pointed out several challenges in cloud forensics, such as the unification of logs format, missing terms and conditions in Service Level Agreement (SLA) regarding investigations where service level agreement is the main point and condition between the user and the cloud

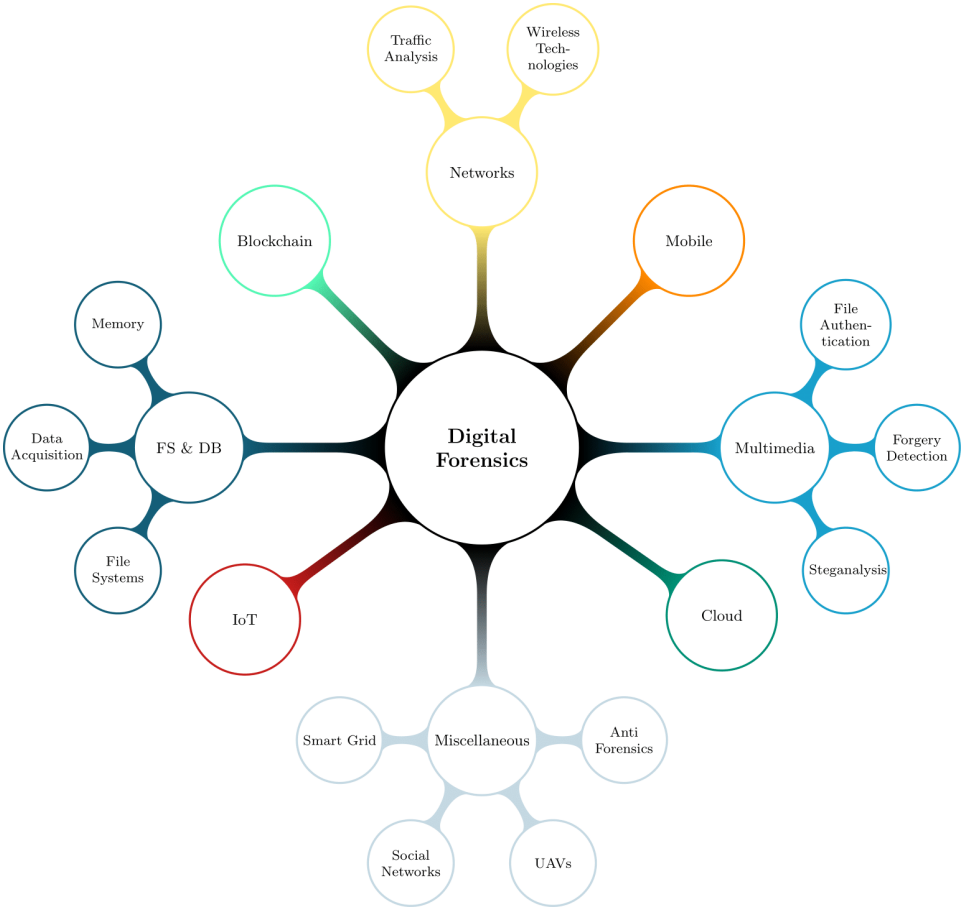

FIGURE 3. Challenges-based and domain-specific mindmap abstraction of digital forensics topics identified in the literature.

service provider, lack of forensics expertise, decreased access to forensic data and control over forensics data at all level from the customer side, lack of international collaboration and legislative mechanism in cross-nation data access and exchange, and lack of international collaboration and legislative mechanism in cross-nation data access and exchange. Pichan *et al.* [26] considered the Digital Investigative Process (DIP) model [27] for describing the challenges emerging at each phase of the digital investigation process and provided solutions for the respective identified challenges. The challenges identified by the authors in cloud forensics are unknown physical location, decentralized data, data duplication, jurisdiction, encryption, preservation, dependence on CSP, chain of custody, evidence segregation, distributed storage, data volatility and integrity. Similar to the works of Khanafseh *et al.* and Pichan *et al.*, the authors in [28] also identified the challenges in cloud forensics and analyzed them on the basis of their significance. Park *et al.* [29] discussed the different challenges within cloud forensic investigations highlighting the relevance of proactive models, and discussing the integration of smart environments to enhance the robustness of forensic investigations. The authors in [30] provided a categorization of the cloud forensic challenges based on the cloud forensic process stages. Amminezhad *et al.* [31] described the different challenges in cloud forensics that were addressed by other authors by performing an exploratory analysis. Rahman *et al.* [32] broadly classified the existing challenges in cloud forensics, classifying the literature into three categories, namely, multi-tenancy, multi-location and scope of user control. Finally, the authors in [33] identified and discussed the major challenges that occur at each stage of the cloud forensic investigation, according to well-known forensic flows.

As evident from the large number of publications in literature reviews/surveys, cloud forensics is quite an explored research topic. Despite the considerable amount of research in cloud forensics, there still exist a number of challenges/limitations that need much attention, as discussed by NIST [34]. In Table 3, we present a summary of the extracted challenges in the cloud forensic review/survey articles. From this summary, we observe that there is a dearth of research work focusing on cloud forensic standard tools and technologies in the cloud environment. Also, very limited works have concentrated on pointing out the feasible solutions related to the challenges present in cloud forensics.

TABLE 3. High level extraction of limitations in cloud forensics.

Challenge/Limitation	References
Update forensic tools to fight novel cybercrime	[7], [25], [26], [29], [30], [33]
Lack of forensic readiness mechanisms and their management	[24], [26], [29], [33], [35]
Data management and its fragmentation hinders investigations	[7], [24]–[26], [28], [30]–[32], [35]
Lack of trust and robust chain of custody preservation	[7], [24]–[26], [28], [29], [35]
Lack of jurisdictional mechanisms for confidential data	[28], [30], [35]
Cross border investigations due to different jurisdictions and laws	[7], [24]–[26], [28]
Lack of training and interoperability between investigators and court	[25]
Anti-forensics	[7]

B. NETWORKS

Data monitoring and acquisition from network traffic are mandatory to prevent most of nowadays cyber-attacks [36]–[38], including, but not limited to, Distributed Denial of Service (DDoS), phishing, DNS tunnelling, Man-in-the-middle (MitM) attacks, SQL injection and others [39], [40]. Regardless of the orchestration mechanism behind them (i.e., single attackers or orchestrated botnets), the analysis and mitigation mechanisms rely on the proper monitoring and analysis of computer network traffic to collect information, evidence and proof of any intrusion detection or vulnerability. For this purpose, several well-known tools exist, such as network forensic analysis tools which provide functionalities such as traffic sniffing, Intrusion Detection Systems (IDS), protocol analysis, and Security Event Management (SEM) [40]–[43]. Nevertheless, one of the challenges of network forensics is to achieve accurate and efficient packet analysis in encrypted network traffic since it is far more challenging than the analysis of unencrypted traffic. As authors stated in [40], [44], utilizing machine learning in packet analysis is evolving into a complex research field that aims to address the analysis of unknown features and encrypted network data streams.

Regarding the research and forensics-related surveys tackling such issues, several reviews recall the primary methodologies and tools for network forensic analysis, such as the works seen in [36], [45], yet they were conducted almost a decade ago. Therefore, taxonomies classifying forensic frameworks suitable for Network Forensics are crucial [40]. An interesting review focusing on the attackers perspective, in terms of attack behaviour and plan identification, as well as prevention mechanisms, can be found in [46]. Finally, some protocol-oriented reviews, analyzing IEEE 802.11 protocol [43], and more recently, 5G networks [42], discuss specific vulnerabilities in their corresponding contexts. In general, the main challenges of network forensics, as identified by the authors in the aforementioned works, are classified in Table 4.

TABLE 4. High level extraction of challenges in network forensics.

Challenge/Limitation	References
Reduce the amount of data required for attack identification	[36], [40], [44]
Heterogeneous data acquisition, integrity and interpretation	[36], [40]–[42], [45]
Ubiquitous environments and cross border data	[40], [42], [45]
Reliable detection of attacks	[36], [40], [42], [45], [46]
Increased possibilities of monitoring mechanisms	[42], [43], [45]
Efficient and accurate analysis of encrypted traffic	[40], [44]

C. MOBILE

Smartphones and mobile devices may contain valuable information for a plethora of investigation purposes. Mobile forensics (MF) is a sub-branch within the digital forensics domain relevant to the extraction of digital evidence from portable and/or mobile devices. Mobile forensics processes could be broken down into the following three categories: seizure, acquisition, and examination/analysis.

The diversity of embedded OSs with shorter product life cycles, as well as the numerous smartphone manufacturers around the world, stand out as significant challenges in the MF domain [47]. In general, MF presents various challenges due to a multitude of reasons. For example, in [48] the authors identify the following limitations for successfully carrying out MF investigations: 1) data-related issues (anonymity-enforced browsing and other anonymity services, and the considerable volume of data acquired during an investigation) 2) forensic tools-related issues (MF research approaches have long focused on acquisition techniques, while minor importance was given to the other phases of MF investigative process) 3) device and operating systems diversity 4) security aspects (development of new and more sophisticated anti-forensic methods from the manufacturers) 5) cloud-related issues (current MF tools do not consider cloud aspects, cloud investigation barriers such as access to forensics data due to multi-jurisdictional legal frameworks, forensics data security) and 6) process automation. It is worth noting that MF faces significant challenges concerning the focus of the overall MF processes. For example, it is not clear whether investigation procedures should be model-specific for each device or should be generic enough to form a standardized set of guidelines applicable to forensics procedures [49]. Another challenge is the need to perform live forensics (mobile device should be powered on) [50]. In addition, an important barrier for actually conducting MF investigations relates to the various networking capabilities of smartphones, which render the overall MF processes difficult to manage, particularly due to the complex structure of the cloud computing environment [51]. Finally, due to the security measures inherent to modern mobile devices, an investigator must actually break into the device using an exploit that will most likely alter the device data. Clearly, the latter violates the Association of Chief Police Officers (ACPO) principle

and introduces numerous procedural issues for a forensic investigation. In Table 5, we provide a classification of MF approaches' current challenges.

TABLE 5. High level extraction of limitations in mobile forensics.

Challenge/Limitation	References
Reduced training and data acquisition overheads	[48], [51]
Diversity of embedded OSs with shorter product life cycles, multitude of smartphone manufacturers	[47]
Heterogeneous data acquisition and interpretation	[48], [50]
Update forensic tools to fight novel cybercrime	[48], [51]
Strong security mechanisms of mobile devices and anti-forensics	[48], [50]
The very nature of mobile phones necessitates the adoption of live forensics approaches	[50]
Lack of trust and robust chain of custody preservation	[48], [50]
Lack of device-based standards and procedural guidelines	[49]
Lack of jurisdictional and legal requirements for different investigation scenarios	[51]

D. IOT

Although significant in terms of improved data availability and operational excellence, the broad adoption of IoT devices and IoT-related applications have brought forward new security and forensics challenges. IoT forensics is a branch of digital forensics dealing with IoT-related cybercrimes and includes the investigation of connected devices, sensors and the data stored on all possible platforms.

According to the literature, several of the current limitations of IoT forensics include the management of different streams of data sources, the complicated three-tier architecture of IoT, the lack of standardized systems for capturing real-time logs and storing them in a valid uniform form, the preparation of highly detailed reports of all information gathered its corresponding representation, the preservation and acquisition of evidence considering its volatility and value of data, and the adoption of routine forensic tasks in the IoT ecosystem [52]–[56]. Data encryption trends also present additional challenges for IoT forensic investigators, and arguably cryptographically protected storage systems is one of the most significant barriers hindering efficient digital forensic analysis [54], [57], [58]. Other studies highlight additional limitations of IoT forensics processes such as interoperability and availability issues related to the vast amount of connected IoT devices [54]–[56], [59], the Big Data nature of the IoT forensics evidence (Variety, Velocity, Volume, Value, Veracity) [55], [58], [60] and the various security storage challenges of IoT forensics evidence, especially when related to biometric data [61]. Finally, various regulatory-related challenges also exist in the IoT forensics domain, particularly issues relevant to the ownership of data in the cloud as defined by region-specific laws [54]–[56], [58], [59]. For instance, service-level agreements stipulating the ''terms of use'' of the cloud resources between the cloud customer and the cloud service provider do not incorporate forensic investigations' provisions. Legislative frameworks adopted in specific regions, such as the GDPR in Europe, also pose significant challenges for IoT forensic investigations, particularly data privacy provisions [53]–[56]. Finally, the use of blockchain and its capability to enhance IoT forensic investigations has been also discussed in [54]. In Table 6 we provide a classification of the current challenges of IoT forensics approaches.

TABLE 6. High level extraction of limitations in IoT forensics.

Challenge/Limitation	References
Heterogeneous data acquisition, integrity and interpretation	[52]–[56], [59], [60]
Lack of training and interoperability between investigators and court	[52], [53], [58]
Forensic process in IoT environment may necessitate all three levels including device level forensics, network forensics, and cloud forensics	[52]
Lack of forensic readiness mechanisms and their ethical management	[52], [53], [55]
Availability of IoT devices due to their resource-constraint nature	[56], [60]
Cross border investigations due to different jurisdictions and laws	[54]–[56], [58]–[60]
Volume of evidence storage and logging-related issues	[53], [54], [56], [58], [60]
Data encryption mechanisms and cryptographically protected storage systems	[54]–[58]
Sound and standardized methodologies, evaluation procedures and benchmarks	[53]–[56], [59], [61]
Update forensic tools to fight novel cybercrime	[53]–[55]
Lack of provision regarding forensic investigations or evidence recovery in service level agreements between service providers and customers	[53]

E. FILESYSTEMS, MEMORY AND DATA STORAGE FORENSICS

Forensic analysis of large filesystems requires efficient methods to manage the potentially large amount of files and data contained in them. System logs are one of the most used information sources to leverage forensic investigations. In [62] the authors provide a review of the publicly available datasets used in operating system log forensics research and taxonomy of the different techniques used in the forensic analysis of operating system logs. The taxonomy is created based on a common investigation format that includes event logs recovery, event correlation, event reconstruction and visualization. Distributed filesystem forensics is even a more challenging task, such as in the case of identifying the malicious behaviour of the attackers by analysing cloud logs [63]. Nevertheless, the accessibility attributes associated with cloud logs impede the goals of investigating such information, as well as other challenges, similar to those extracted in Section III-A.

Another challenging area is the analysis of proprietary systems such as SCADA systems. In [64] the authors present a survey on digital forensics that are applied to SCADA systems. The survey describes the challenges that involve

applying digital forensics to SCADA systems as well as the range of proposed frameworks and methodologies. The work also focuses on the research that has been carried out to develop forensic solutions and tools that can be tailor-made for the SCADA systems. Recent research has revealed that malware developers have been using a broad range of anti-forensic techniques and escape routes in-memory attacks and system subversion, including BIOS and hypervisors. In addition, code-reuse attacks such as returned oriented programming pose a serious remote code execution threat. To neutralise the effects of malicious code, specific techniques and tools such as transparent malware tracers, system-wide debuggers were proposed. In [65], authors present a survey on the state-of-the-art techniques that demonstrate the capability of thwarting the anti-forensic strategies previously mentioned.

Memory forensics refers to the forensic analysis of a system's memory dump. A system's memory can contain evidence related to the usage of the system, including the list of running processes, network connections, or the keys for the driver's encryption. Usually, such data are not stored in the permanent storage of the system and are completely lost when the system is turned off or unplugged from the power. In the literature, we can find surveys devoted to the analysis of the memory acquisition techniques [66], [67] (i.e., both hardware and software-based), the subsequent memory analysis [68], and the available tools [67]. The main challenges of memory forensics derive from the fact that memory is volatile, so it has to be acquired when the system is running and thus probably modified by the running applications. This can lead to the page smearing issue [68], i.e., inconsistencies between the state of the memory as described by the page tables compared with the actual contents of the memory. Another issue that can occur during the memory acquisition is the incorporation of pages, which are not present in the memory due to page swapping or demand paging [68]. Finally, although the memory acquisition techniques should be OS and hardware agnostic [66], each OS architecture handles the memory differently and is equipped with distinctive tampering protection mechanisms that hinder access to memory.

A database (DB) is the most traditional way to organise and store data. The majority of applications and online services deploy some type of DB to store records about their customers, financial records, inventory, etc. Besides the vast amount of data that could be contained in a DB, a database management system (DBMS) which allows the end-users to administer the DB and store and access the data in a specific format, can also provide evidence of actions in user-level granularity. For instance, it can reveal who and when stored/accessed specific records. Therefore, digital forensics for DB has attracted the attention of the research community [69]. From this perspective, several surveys focused on database digital forensics based on the log files, metadata, and similar types of artefacts for the case of relational and NoSQL DB [70]–[72]. Furthermore, other authors addressed the digital forensic opportunities on the procedure of data aggregation and analysis, as well as their structural architecture to benefit forensic procedures [69], [73]. Digital triage is of special relevance here since reviewing many potential sources of digital evidence for specific information by using either manual or automated analysis is mandatory to enhance investigations [73]. Nevertheless, the authors highlight that the legitimacy of several acquisition procedures is constrained by the applicable legislation and that the current state of practice requires more efficient solutions, especially when dealing with huge amounts of data. In [74], the authors presented a framework for database forensic investigations enhanced by forensic experts' opinions with the aim to overcome the main issues that investigator's face, such as the lack of standardized tools and different data structures and log structures.

Considering the increasing amount of IoT technologies and small devices that require live data analysis due to the volatility of the data stored in them, it is crucial to develop new strategies to enhance data acquisition procedures [75]. In the context of database forensics and data acquisition, the challenges of big data analysis and data mining techniques for digital forensics [76], [77], and text clustering [78] were investigated. Moreover, a survey of techniques to perform similarity digest search is provided in [79].

Table 7 summarises the main limitations and challenges extracted from the literature analysed in this section.

TABLE 7. High level extraction of challenges in file system, memory and data storage forensics.

Challenge/Limitation	References
Performance issues and logging inducing overhead in terms of query latency, storage, etc.	[62], [65], [70], [71], [73], [79]
Lack of standardized tools and technologies	[63], [69], [70], [73], [74], [78]
Forensic seizure and analysis of proprietary and/or distributed filesystems	[62]–[64], [74], [75], [75], [77]
Variety of format and content type. Not standard logging features and settings	[65], [69]–[74], [77], [79]
No validation/verification in real-life scenarios and large datasets	[76], [78]
Subjectivity of the evaluation of content retrieval algorithms	[76], [78]
Advanced knowledge and training of analysts and investigators	[73], [76]
Lack of guidance for investigators regarding selective search and seize. Subjectivity of search terms based on investigator's experience	[73], [78]
Difficulty to apply low-level analysis techniques, hindering correctness of the results	[66], [74]
Sophisticated malware implementing anti-forensic techniques	[65]–[67], [78]
Volatile data acquisition due to hardware constraints	[75]
Stealthy non-memory-resident malware	[68]
Handling, execution and monitoring of memory	[65], [67], [68]
Physical access to RAM	[66], [75]
Accurate similarity search of documents and Dynamic insertion/deletion of elements	[79]

F. BLOCKCHAIN

Blockchain technology has been constantly integrated into existing systems or used as the basis to rebuild systems from

scratch in various domains. Besides the financial domain to which it was initially applied, through bitcoin, blockchain technology is currently used in various other use cases such as supply chain management, cybersecurity enhancement, document/certificates validation, crowdfunding campaigns, and more [80]. Additionally, because financial system set on blockchain provide more privacy than traditional payment systems, it is common for cryptocurrencies to be used for criminal activities [81]. This sets blockchain forensics methodologies as a necessity [82] due to the large volume of data that are stored in blockchain systems and the number of processes that are managed by such systems. The main property of blockchain-based systems is the guaranteed protection of data integrity, which is directly related to forensic analysis. On the one side, this property makes forensic analysis more manageable. However, on the other side, this may complicate the process as users may be more cautious when interacting with such systems.

It has to be noted that a large portion of blockchain systems are public, allowing access to everybody and thus making forensic analysis a surplus process. A forensics investigator can set up a node in a public blockchain network, sync it with the rest of the nodes and obtain a local copy of the ledger. Even in such cases, the structure of the information stored in the ledger of blockchain systems is not optimal with respect to retrieving all required data (e.g., for a specific account or a specific smart contract), so efficient mechanisms are required [83] to extract valuable information out of the large volume of data stored in public ledgers [84]. In the case of private blockchain systems, the ledger data are not publicly available and traditional forensics approaches have to be applied to blockchain nodes to extract data.

Even if data are by default publicly available, it is still challenging to identify malicious activity on such platforms. It is common for deployed smart contracts to suffer from various vulnerabilities either due to poor implementation or not properly configured blockchain networks [85]. In such cases, users can take advantage of such vulnerabilities, mainly aiming at financial profit. It is challenging to detect such activity and identify the actors that have initiated it. Smart contracts execution is not a straightforward process, and past execution cannot be easily repeated in a forensic sound way [86]. Apart from that, smart contracts may also get self-destructed by a special OPCODE that makes following past transactions even harder [87].

Furthermore, privacy concerns have been raised concerning early open public blockchain systems, and thus, there have been multiple alternative systems that make use of various privacy-enhancing techniques such as zero-knowledge proofs, onion routing or ring confidential transactions to protect users privacy [88]. In such cases, forensics analysis of either network nodes or users' wallets is required to retrieve either logs or cryptographic keys that can be used along with data existing on public ledgers and provide more information about the transactions that have taken place.

While the data stored in the ledger are of great importance, there are more data to be considered when analyzing a blockchain node. The ledger holds all committed transactions, but a blockchain node stores more information with respect to its interactions with other nodes or clients. For example, the IP of the client that has connected to a node to submit a transaction or the activity of a specific node in the network (e.g., sync requests) are not included in the ledger's data. On top of those, multiple security blockchain attacks are mainly targeted against the infrastructure or the network's backbone and not against its content. Mining attacks, network and long-range attacks [89], [90] target at taking control of the blocks formation process, to maliciously alter past committed transactions and achieve double-spending attacks. In such cases, digital evidence from deployed nodes is the only way to prove malicious activity. At the same time, the size of the network in public blockchain systems makes it even harder to retrieve the required evidence. Table 8 summarises the main challenges extracted from the blockchain forensics literature.

TABLE 8. High level extraction of challenges in blockchain forensics.

Challenge/Limitation	References
Acquisition of large volume of data	[83], [84]
Inefficient data structures and lack of standardized analysis	[83]
Privacy preserving mechanisms that hinder data acquisition	[88]
Difficulties in exploring smart contracts execution	[85]–[87], [89]
Mining and network attacks	[89]

G. MULTIMEDIA

Due to the increasing number of ubiquitous technologies (e.g., IoT devices, smartphones, wearables) leveraged by the 4^{th} industrial revolution, as well as a substantial improvement in the connectivity capabilities in smart scenarios due to 5G, the amount of multimedia prosumers (i.e., both producers and consumers of data) is increasing dramatically year after year.[2] Nevertheless, such multimedia content growth is a double-edged sword. On the one hand, it is a synonym of opportunities for the industry, companies and users. On the other hand, it augments the possible vulnerabilities and attack vectors of such systems, which malicious users can exploit.

Digital forensics in the context of multimedia has received substantial attention from the research community. There exist numerous image forgery detection surveys exploring the topic from a global perspective [91]–[99]. In this context, pixel-based image forgery detection is one of the main topics [100], including image splicing forgery [101], and copy-move forgery [102]–[104], which is a well-known technique in which parts of the current images are used to cover/hide specific characteristics. Some authors focused on

[2]https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

TABLE 9. High level extraction of challenges in multimedia digital forensics.

Challenge/Limitation	References
Standardized evaluation procedures and benchmarks	[94], [98]–[100], [102], [104], [105], [108], [113]–[118], [120], [121], [127]
Explore the use of novel AI methods and novel data types	[92], [95], [97], [99], [103], [104], [107], [108], [110], [111], [113], [114], [116], [117], [119], [122], [125]–[128]
Robust pre-processing and feature extraction	[94], [95], [98], [101], [103], [105], [106], [109], [110], [113], [119], [121], [122], [125], [127], [128]
Reduce training and data acquisition overheads	[93], [95], [97], [99], [110], [114]–[116], [118], [122], [123], [125]
More comprehensive outcome readability	[94], [97], [103], [105], [115], [119], [120]
Increased effort to circumventing anti-forensic techniques	[91], [94], [95], [100], [105], [113], [115], [119], [122], [124], [127]
Rigorous mechanisms to ensure protection/watermarking	[100], [108]
Analyse multiple threats/tampering at once	[94]–[96], [99], [100], [111], [112], [114], [116], [117], [120], [123], [127]
Reliable detection with real data and dynamic contexts	[95], [114], [124]

passive techniques to detect forgery [105], or carving on specific file formats such as JPEG [106]. Other image forensics surveys analysed topics such as hyperspectral image [92], [107], image authentication [108], the affectation of noise in images [109] and image steganalysis [110]–[114]. Another set of surveys focus on the specific context of child abuse material and its detection through image and video analysis [115]–[118]. More recently, the advent of deep learning techniques has enhanced the capabilities of image integrity detection and verification, outperforming traditional methods in several image-related tasks, especially in these where anti-forensic tools were used [113], [114], [119]. In the context of video files, we can find surveys on video steganalysis [113], [114], [120], video forgery detection [95], [96], [98], [114], [121], [122], video forensic tools [95], [113], [123], [124], video surveillance analysis [125], [126], and video content authentication [127]. Finally, digital audio forensics has also been studied in [128]. Table 9 summarises the main limitations and challenges extracted from the multimedia forensic literature.

H. MISCELLANEOUS

This section is devoted to the digital forensics reviews that fall beyond the domain categorisation of the previous paragraphs.

As observed in most topics, anti-forensics can be understood as a standalone concern in digital forensics, which requires investigation in each context. The term anti-forensics refers to methods and strategies that prevent forensic investigators and their tools from achieving their goals. There are several examples of anti-forensic methodologies [129], such as encryption, data obfuscation (e.g., trail obfuscation), artifact wiping, steganography and image tampering [130], protected/hidden communications (e.g., tunnelling, onion routing), malware anti-sandbox/debug, VM and in general anti-analysis methods [131]–[134], and spoofing. As stated in [135], anti-forensic methods exploit the dependence of human elements on forensic tools, as well as the limitations of the underlying hardware in terms of architecture and computational power. Therefore, enhancing the training and knowledge level of investigators and more robust forensic procedures (e.g., anti-anti forensic techniques [130]) are critical to minimise the impact of anti-forensics. In this line, some authors argue that the use of proactive forensics models could help enhancing the robustness of forensic investigations [136].

Another emerging topic in digital forensics is related to unmanned aerial vehicles (UAVs), or more commonly known as drones [137]. The applications and versatility of these devices are becoming more popular in a myriad of contexts, from industrial to military applications. One of the main challenges of drone forensics is the set of different hardware components that are part of a drone [138], and the particular treatment that they require (i.e., with special regard to advanced anti-forensic techniques taking place [139], as well as the necessity of live forensics [137], [140] in this context). For instance, drones consist of sensors, flight controllers, electronic and hardware components, on-board computers, and radiofrequency receivers, each one linked to one or many evidence sources in terms of, e.g., data storage (the different memory sources present in the drone, such as memory cards storing media, or other software), data communications and other logs and data stored in sources related to the drone, such as the drone controller and external cloud-based sources [141], [142]. At the moment of writing, there are no baseline principles, standards, nor legislation covering all the particularities of forensic drone investigations [137], [142]. Thus, efforts towards the establishment of sound protocols, specific forensic frameworks, as well as drone-based forensic tools are critical [137].

In [143], authors surveyed the different dimensions and concerns which digital forensics should cover in the context of social networks. The authors discussed several aspects of social networks, such as privacy and security issues, the criminal and illegal acts that can occur, and the attacks on the underlying platform and the users. In addition, they describe several strategies to detect such abnormal behaviours along with the necessity to develop both pro-active and reactive mechanisms. In terms of community detection, graph analytic methods and tools are crucial to detect criminal networks in different contexts, such as finance, terrorism, and other heterogeneous sources [144]. In [8], authors surveyed the efforts done so far on the analysis of social network shared data according to source identification, integrity verification and platform provenance. Moreover, authors discussed the current methodologies, and highlighted the current challenges

along with the need for multidisciplinary approaches to overcome them.

A sector that is receiving increasing attention due to its critical relevance to the proper functioning of our society is the energy sector, and more concretely, the smart grid. In [145], authors explore practical cybersecurity models and propose some guidelines to enhance the protection of the smart grid against cyber threats. Moreover, they explore software-defined networks and their main benefits and challenges. Finally, the authors propose a conceptual forensic-driven security monitoring framework and highlight the relevance of forensics by design in development phases. Context-aware scenarios such as smart cities have been also receiving increased attention due to their complex structures, requiring the continuous data collection, processing and interaction between a myriad of devices [146], [147]. Digital forensics in this particular scenario is a recent paradigm which requires further efforts from the research community to enhance cyber resilience and to provide efficient incident response mechanisms [147].

I. CHALLENGE ANALYSIS AND AGGREGATED RESULTS

The classification of challenges and limitations according to each topic of the taxonomy has been conducted to keep a balance between accurate descriptions of challenges and hierarchical classification. On the one hand, we want to facilitate identifying the gaps and limitations of each topic and provide a clear path for both new and experienced investigators towards the corresponding literature. On the other hand, and as stated in Section I, we provide the reader with a clear overview of the research lines that should be strengthened in the digital forensics ecosystem, as well as their interrelations according to each topic of our taxonomy. Therefore, we used the extracted challenges of each topic and merged the ones appearing more than once (i.e., the ones appearing only in their corresponding topic were ignored due to their specificity) to create a comprehensive overview of the digital forensics challenges in Table 10. As it can be observed, we identified several limitations of digital forensics that can be applied in several topics or contexts and thus, indicate the need to devote more research efforts towards them. Note that, for instance, the last topic of the Table 10 appears to be only affecting IoT, yet we identified this challenge in the miscellaneous topic, and thus, we decided to include it. Nevertheless, since several topics are analysed in such a category, we did not represent them in Table 10.

The most reported challenge is the sound data acquisition from heterogeneous sources and its interpretation, including different hardware and monitoring processes collecting data and logs dynamically. Note that data acquisition and management is a challenge affecting activities related to digital forensics. Moreover, data fragmentation, a common scenario nowadays, hinders investigations further. It is important to note that data acquisition is critical to creating benchmarks, which help researchers and practitioners to evaluate their models. The latter enables characteristics such as reproducibility and pushes the advancement in the state of the art, which is needed to keep up with the pace of technology development [148], [149]. The next most challenging issue is related to anti-forensics methods, which has been discussed in several sections of the taxonomy as well as in Section III-H. Anti-forensic strategies leveraged by malicious actors include adversarial methods such as obfuscation or encryption applied to, e.g., data and storage systems, as well as hardware-related technological challenges, such as mobile phones due to their inherent security measures, or in the case of drones due to their specific particularities, and software, as well as in the case of malware. In the case of tools and evaluation benchmarks, it is evident that the community needs to devote more efforts towards fighting novel cybercrime, especially in topics where, e.g., different data sources and technologies are present. For instance, in the case of IoT and UAVs, different data sources may necessitate different digital forensics strategies, including tools related to device level forensics, network forensics, and cloud forensics. Another challenge that affects digital forensics is the lack of jurisdictional and legal requirements for different investigation scenarios such as ethics and data management of confidential and personal data. This is particularly relevant nowadays due to the widespread use of distributed systems such as blockchain and the cloud. The latter means that software and data may reside in different countries, and thus, specific cross-border collaborations are required, adding another layer of complexity to digital investigations. Moreover, this scenario impedes the adoption of proactive measures due to the difficulty of applying measures that conform to different legal frameworks.

A proper understanding between all the actors involved in the digital forensics context, including stakeholders, LEAs, and court members, is mandatory to ensure the successful prosecution of perpetrators. In this regard, one of the highlighted challenges is to ensure that all partners have a sufficient level of training (including technical knowledge and standardised guidelines) and a proper understanding, including readable reports to enable a fruitful collaboration. Moreover, while it seems procedural, the chain of custody is still a challenge. This can be attributed to multiple reasons, such as obvious negligence of the corresponding personnel to properly report evidence acquisition and/or handling, corrupted officers, or even gaps in the process. Nevertheless, all of them cause severe issues in a court as a case can be missed or misjudged. Secure and auditable means of storing and processing the chain of custody, as proposed by LOCARD[3] with the use of blockchain technology seems like a logical and stable solution. A more thorough description of forensic readability and its challenges is discussed later in Section IV-C.

Data acquisition, as previously stated, is not only a challenge in terms of the existing heterogeneous data sources and context but also in terms of size. The big data era comes with a myriad of opportunities but also with their corresponding

[3]https://locard.eu/

TABLE 10. Cross-domain abstraction of the challenges and limitations of digital forensics, ordered by relevance according to the amount of times they were found in the topics of the taxonomy. For the sake of fairness, the general column *Miscellaneous* has been omitted.

Challenge/Limitation	Cloud	Networks	Mobile	IoT	FS & DB	Blockchain	Multimedia
Sound data acquisition from heterogeneous/ubiquitous sources	✓	✓	✓	✓	✓		✓
Anti-forensics and protected storage systems	✓		✓	✓	✓	✓	✓
Sound and standardized evaluation procedures and benchmarks				✓	✓	✓	✓
Lack of jurisdictional and legal requirements for different investigation scenarios	✓		✓	✓			
Lack of forensic readiness mechanisms and their management	✓			✓			✓
Update forensic tools to fight novel cybercrime	✓		✓	✓			✓
Lack of training and interoperability between investigators and court	✓			✓	✓		
Reduce pre-processing, training and data acquisition overheads		✓	✓			✓	✓
Cross border investigations due to different jurisdictions and laws	✓			✓			
Lack of device-based standards and procedural guidelines			✓		✓		
Reliable detection of threats/attacks and testing in real scenarios		✓			✓		✓
The nature of the devices requires the adoption of live forensics approaches			✓	✓	✓		
Evidence storage and logging-related issues				✓	✓		
Multiple forensic contexts due to different data sources				✓			
Lack of trust and robust chain of custody preservation	✓		✓				
Availability of devices due to their resource-constraint nature				✓			

challenges, since logging and data acquisition in specific scenarios may pose technical challenges. This issue is exacerbated when coupled with cross-border investigation requirements due to data fragmentation. Moreover, once data corresponds to multiple forensic contexts, the complexity of performing digital investigation grows exponentially, leaving aside the need to perform live forensics according to the particularities of the hardware. Additionally, the availability of some devices due to their resource-constraint nature is a further challenge. For instance, IoT botnets have high volatility, and UAVs may implement self-defence mechanisms, even at the physical level. In the case of the *Miscellaneous* category, we included the challenges and limitations of anti-forensics, drone forensics, smart grid, smart cities and social networks.

According to the outcomes depicted in Table 10, we can observe that topics such as IoT, cloud, and mobile are affected by the highest amount of challenges. Therefore, we believe that researchers and practitioners should devote more efforts to solving such topics' challenges by leveraging cross-domain collaborations to enhance the quality and applicability of their outcomes. Similarly, other challenges which appear in several topics could be tackled more quickly if they were targeted with a multidisciplinary approach, with experts from the different digital forensics topics.

To create a visual representation of these challenges, we believe that mapping each challenge into different categories will highlight which need to be reinforced. Therefore, Figure 4 presents the outcomes of our taxonomy in terms of topic challenges mapped into different categories representing different phases, from the creation of the legal basis and framework of an investigation to the final reporting of the outcomes. As it can be observed, the challenges most cited in the literature are present in the evidence acquisition and data pre-processing category. They are mainly related to data acquisition issues and anti-forensics. Notably, these challenges affect the forensic procedures from the beginning (i.e., if we do not consider the standards, legislation and procedural category), and thus, it is crucial to devote efforts to overcome them. The investigation and forensic analysis category contains the highest number of challenges. Therefore, the topics identified in the taxonomy share similar technical concerns in their corresponding contexts, and more multidisciplinary collaboration is needed towards such direction. The reporting and presentation category highlights one yet critical challenge since the proper reporting of an investigation affects the outcome of the whole investigation. We further discuss about forensic readability and reporting in Section IV-C.

IV. DIGITAL FORENSICS METHODOLOGIES, PRACTICES AND STANDARDS

In addition to the topic-based taxonomy presented in Section III, we collected a set of literature reviews, included in our research methodology, that analysed forensic frameworks and process models, and the adaptability and forensic readiness of the actual practices. In the following sections, we analyse the content of such reviews by extracting the challenges and identifying the main qualitative features required to achieve forensically sound investigations.

A. FORENSIC FRAMEWORKS AND PROCESS MODELS

A digital forensics framework, also known as a digital forensics process model, is a sequence of steps that, along with the corresponding inputs, outputs and requirements, aim to support a successful forensics investigation [150], [151]. A digital forensics framework is used by forensics investigators and other related users to ease investigations and the identification and prosecution of perpetrators. In addition to a set of specific steps identifying each investigation phase, the use of digital forensic frameworks enables timely investigations, as well as a proper reconstruction of the timeline of events and their associated data. In this regard, one of the most critical aspects of a digital investigation is the proper preservation of the evidence chain of custody, since it could lead to unsolvable inconsistencies, risking the admissibility of evidence in court.

According to their phases and their granularity, there are different investigation models suitable for different types

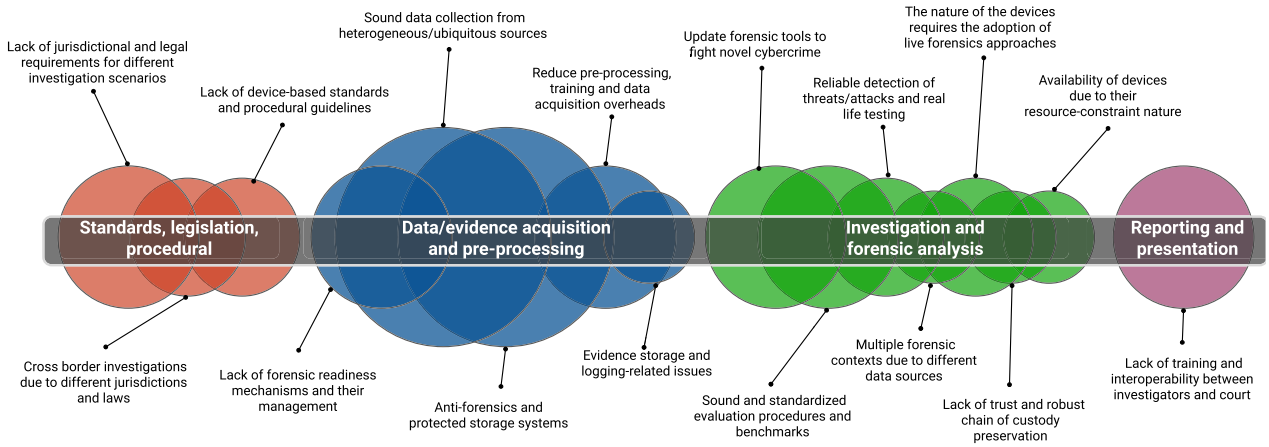

FIGURE 4. Main digital forensic challenges mapped into different categories according to their application context, from the initial steps of an investigation (left) to the final ones (right). The size of each circle denotes the times it appeared considering the topics of the taxonomy.

of investigations. In this regard, Kohn *et al.* provide [152] an integrated suitability framework that maps a set of requirements derived from an ongoing investigation to the most suitable forensic procedure. Moreover, the authors also use a graph-based approach to associate the most well-known forensic frameworks and their interrelationships regarding the number of phases and their content. Other well-known frameworks include the Analytical Crime Scene Procedure Model (ACSPM) [153], the Systematic digital forensic investigation model (SRDFIM) [154], and the advanced data acquisition model (ADAM) [155]. In general, law enforcement agencies follow variants of the ACPO (Association of Chief Police Officers) guidelines [156]. Finally, other forensic guidelines and models proposed by NIST and INTERPOL can be found in [5], [157]. The most well-known digital forensic frameworks are summarised in Table 11.

In general, the procedures summarised in Table 11 have a common hierarchical structure [165], [166], which can be divided in the steps described in Table 12. Note that some of the models may include more granular approaches to some of the steps, which are necessary due to the investigation context (e.g., specific devices and seizure/acquisition constraints).

In the case of the chain of custody and trail of events preservation, a forensically sound procedure needs to ensure features such as integrity, traceability, authentication, verifiability and security [167], [168]. In this regard, Table 13 provides a description of each feature.

In the past, several authors identified several challenges in digital investigation processes [77], [169]–[175], mainly related to the chain of custody preservation, the growth of the data to be processed, and privacy and ethical issues when collecting such data. In addition, our research methodology identified several literature reviews which discussed the challenges and limitations of forensic frameworks. For instance, in [176], the authors leveraged a summary of digital forensic frameworks and tools as well as their interrelationships by using a graph analysis methodology. In addition, they discussed some challenges and limitations of privacy-preserving digital investigation models and proposed some measures to palliate them. In [177] the authors presented a chronological review of the most well-known forensic frameworks and their characteristics. The work presented in [178] evaluates the current frameworks among European law enforcement agencies, identifying and defining elements of robustness and resilience in the context of sustainable digital investigation capacity so that organisations can adapt and overcome deviations and novel trends. In [175], the authors identified the need to define specific models according to the forensic context, such as in the case of Mobile Forensics [175]. Moreover, the authors proposed a specific forensic framework to improve Mobile Forensics investigations. Further reviews of the most used forensic frameworks and their features can be found in [179], [180]. Table 14 reports the main challenges in forensic frameworks identified by each literature review.

In parallel to forensic guidelines and frameworks, standards are crucial to ensure conformance and mutual compliance across geographical and jurisdictional borders. There are currently numerous standards and established practices provided by organisations worldwide using accepted methods. The technical details on how to forensically approach a given investigation differ depending on the device. The analysis of electronic evidence is typically categorised into the phases stated in Table 12. However, the exact phases naming may vary due to different forensic models' usage according to each organisation's needs.

While not an official standard, the Cyber-investigation Analysis Standard Expression (CASE)[4] is a community-driven standard that aims to develop an ontology that can efficiently represent all exchanged information and roles within the context of investigations regarding digital evidence. The International Organization for Standardization (ISO) has released a series of standards to assist in this effort by providing the family of ISO 27000, focusing on information security standardisation procedures. In what follows,

[4]https://caseontology.org/

TABLE 11. Most well-known forensic models and guidelines.

Name	Year	Reference
Digital Forensic Investigation Model	2001	[158]
Digital Investigative Process Model	2001	[27]
Abstract Digital Forensic Model	2002	[159]
Integrated Digital Investigation Model	2004	[160]
Enhanced Digital Investigation Process Model	2004	[161]
Extended Model of Cybercrime Investigation	2004	[162]
NIST Guide to Integrating Forensic Techniques into Incident Response	2006	[157]
Digital Forensic Model for Digital Forensic Investigation	2011	[163]
Systematic digital forensic investigation model	2011	[154]
ACPO guidelines	2012	[156]
Analytical Crime Scene Procedure Model	2013	[153]
Advanced data acquisition model	2013	[155]
INTERPOL Guidelines for Digital Forensics Laboratories	2019	[5]
ENFSI Guidelines	2016-2020	[164]

TABLE 12. Main steps in a digital forensic investigation model.

Forensic Step	Description
Identification	Assess the purpose and context of the investigation. Initialize and allocate the resources required for the investigation, such as policies, procedures and personnel.
Collection & Acquisition	The seizure, storage and preservation of digital evidence. Although this two steps need to be strictly differentiated in the physical forensics context, a more relaxed approach can be considered in the digital context.
Analysis	The identification of tools and methods to process the evidence and the analysis of the outcomes obtained
Reporting & Discovery	The proper presentation of the reports and information obtained during the investigation to be disclosed or shared with the corresponding entities, including the court.
Disposal	The relevant evidence are either properly stored for future references or erased. In specific cases, evidence are returned to the corresponding owners.

TABLE 13. Main features required to guarantee chain of custody preservation.

Feature	Description
Integrity	The events data as well as evidences cannot be altered or corrupted during the transferring and during analysis.
Traceability	The events and evidence can be traced from their creation till their destruction.
Authentication	All the actors and entities are unique and provide irrefutable proof of identity.
Verifiability	The transactions and interactions can be verified by the corresponding actors.
Security	Only actors with clearance can add content to an investigation or access to it.

we present the most relevant standards about digital forensics investigations, which are summarised in Figure 5.

ISO/IEC 17025:2017: In some terms, this standard can be considered an ''infrastructure'' standard for forensic labs. It defines the managerial and technical requirements that testing and calibration laboratories must conform to ensure technical competence and guarantee that their test are calibration results are acceptable by the corresponding suppliers and regulatory authorities.

ASTM E2916-19: The goal of this standard is to assemble the necessary technical, scientific and legal terms and the corresponding definitions in the context of the examination of digital and multimedia evidence. Therefore, the standard spans to various areas such as computer forensics, image, audio and video analysis, as well as facial identification. As a result, ASTM E2916-19 creates a common language framework for all.

ISO 21043-2:2018: This standard specifies many requirements for the forensic processes in focusing on recognition, recording, collection, transport and storage of items of potential forensic value. It includes requirements for the assessment and examination of scenes but is also applicable to activities that occur within the facility. This document also includes quality requirements.

ISO/IEC 27035: This is a three-part standard that provides organisations with a structured and planned approach to the management of security incident management covering a range of incident response phases

ISO/IEC 27037:2012: This standard provides general guidelines about the handling of the evidence of the most common digital devices and *the circumstances including devices that exist in various forms*, giving the example of an automotive system [181].

ISO/IEC 27038:2014: Describes the digital redaction of information that must not be disclosed, taking extreme care to ensure that removed information is permanently unrecoverable.

TABLE 14. High level extraction of challenges reported in forensic frameworks literature reviews.

Challenge/Limitation	References
Privacy and ethical data management	[176]
Seize and investigate big volumes of data	[174]–[176], [178]
Cross-border models and chain of custody preservation	[176], [178]–[180]
Adaptable frameworks for novel cybercrime campaigns	[175], [177], [178], [180]
Effective reporting readability and complexity	[174], [178]
Training and collaboration between stakeholders involved in forensic investigation and prosecution	[178]
Cross-domain technical challenges, technologies, anti-forensics	[175], [179], [180]

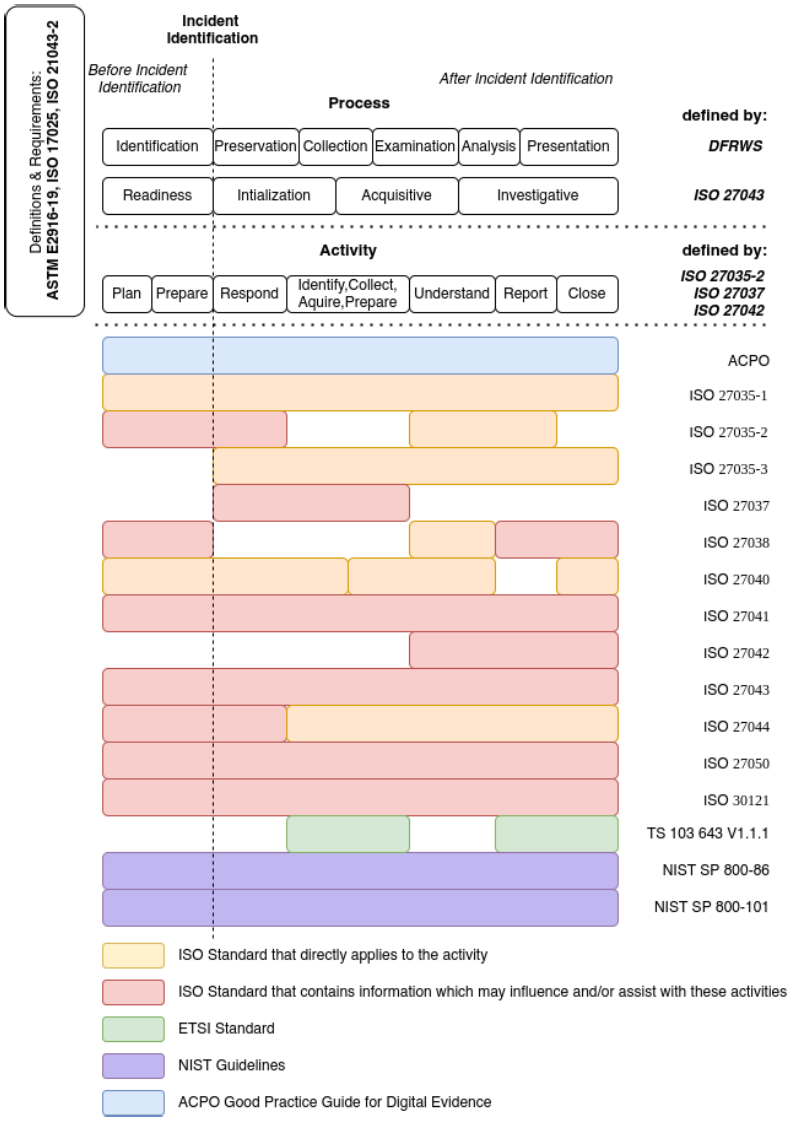

FIGURE 5. **Applicability of standards and guidelines to the investigation process classes and activities.**

ISO/IEC 27040:2015: Provides detailed technical guidance on how organisations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security.

ISO/IEC 27041:2015: Describes other standards and documents to provide guidance, setting the fundamental principles ensuring that tools, techniques and methods, appropriately selected for the investigation.

ISO/IEC 27042:2015: This standard describes how methods and processes to be used during an investigation can be designed and implemented to allow correct evaluation of potential digital evidence, interpretation of digital evidence, and effective reporting of findings.

ISO/IEC 27043:2015: It defines the key common principles and processes underlying the investigation of incidents and provides a framework model for all stages of investigations.

ISO/IEC 27050: This recently revised standard guides non-technical and technical personnel to handle evidence on electronically stored information (ESI).

ISO/IEC 30121:2015: Provides a framework for organizations to strategically prepare for a digital investigation before an incident occurs, to maximise the effectiveness of the investigation.

ETSI is a European Standards Organization that produces standards for ICT systems and services used worldwide, collaborating with numerous organisations. In 2020, ETSI published TS 103 643 V1.1.1 (2020-01) [182], a set of techniques for assurance of digital material in a legal proceeding,

to provide a set of tools to assist the legitimate presentation of digital evidence.[5] In the meantime, the National Institute of Standards and Technology (NIST) has released guidelines for organisations to *develop forensic capability* (see also Table 11), based on the principles of forensic science in the aspect of the application of science to the law. Still, it should not be used on digital forensic investigations due to subjection to different laws and regulations, as clearly stated in their manual. The scope of NIST guidelines is *incorporating forensics into the information system life cycle* of an organisation. The most relevant guidelines are 800-86 [183] for Integrating Forensic Techniques into Incident Response and 800-101 [184] for Mobile Device Forensics.

The Scientific Working Group on Digital Evidence (SWGDE) is an organisation engaged in the field of digital and multimedia evidence to *foster communication and cooperation as well as to ensure quality and consistency within the forensic community*. SWGDE has released several documents to provide the current best practices on a large variety of state of the art forensics subjects. Nonetheless, none of them is targeting or addressing drone forensics's particularities. Finally, a review of the international development of forensic standards can be found in [185].

B. FORENSIC READINESS

In the past, forensic investigations leveraged a post-event approach, mainly focusing on the analysis of data related to a past incident. In this regard, forensic readiness in terms of pro-active techniques and protocols appeared to minimise the cost and the impact of incidents and are widely used nowadays [15], [186]–[188].

We can find different research approaches, such as the review conducted in [189], in which authors discussed how to achieve forensic readiness by collecting the opinion of experts to elaborate a readiness framework with which improve forensic investigations from an organizational perspective. In the case of [190], authors discussed forensic readiness and several procedures to achieve it, such as fostering the use of Trusted Platform Modules (TPM). Other authors reviewed measures to achieve forensic readiness in a holistic way [15], [191]–[194], as well as recalling the relevance to include and expand the actual guidelines towards incident response readiness (e.g., as in the drafts of the ISO/IEC JTC 1/SC 27 working groups, and the ISO/IEC 27035), training and collaboration between stakeholders involved in forensic investigations and prosecution, and effective reporting readability and complexity. Table 15 describes the main forensic readiness challenges identified by the authors in the literature.

Finally, in Table 16 we provide a qualitative summary of the literature reviewed in IV according to the topics discussed in each article. From Table 16 we can see that topics such as privacy and ethics and the suitability of frameworks that are being proposed to fight novel cybercrime need to be further discussed in the literature. Nevertheless, as previously stated in the article, one of the main challenges is that cybercrime evolves faster than countermeasures and legislations, and thus, investigators are always one step behind.

[5]https://www.swgde.org/documents/published

TABLE 15. High level extraction of challenges reported in forensic readiness literature reviews.

Challenge/Limitation	References
Privacy and ethical data management from heterogeneous sources	[15], [195]
Cross-border models and interoperability	[15], [189]–[191], [193]–[195]
Effective reporting readability and complexity	[189], [190], [192], [193]
Training and collaboration between stakeholders involved in forensic investigation and prosecution	[15], [190], [191], [194], [195]
Cross-domain technical challenges, technologies, anti-forensics	[15]

C. FORENSIC READABILITY AND REPORTING

The continuous appearance of novel ICT technologies, paired with discovering new vulnerabilities and attacks that threaten them, dramatically increases the amount of information collected during forensic investigations. The latter refers to the amount of data collected from devices and systems, as well as the heterogeneous data structures required in each case and the specific forensic methodologies developed to detect such threats. In this context, creating interoperable and auditable forensic procedures is a hard task, especially due to the lack of standardised reporting mechanisms. Moreover, qualitative aspects such as the outcomes and conclusions supported by the forensic analysis are often not reported accurately in an attempt to balance between technicality and comprehensibility, hindering the robustness of the findings [14], [198], [199]. Of particular relevance is the communication and readability of such reports, especially if these are to be interpreted by law practitioners, judges, and other stakeholders who do not always have the necessary technical background about the forensic tools nor the underlying technologies analysed [200], [201]. The latter issue has been extensively analysed according to different approaches, from lexical density and complexity [202]–[208], to cognitive and psychological features [209], [210], showcasing the need to improve the reporting mechanisms and the possible benefits of a common, standardised framework. In addition to such a framework, it is crucial to develop the corresponding training procedures for its adoption [211].

It is necessary to recall that the admissibility of a piece of evidence and the forensic validation in court is mandatory to the proper prosecution of perpetrators and constitute the culminating point of an investigation [212], [213]. Therefore, several authors collected the challenges and issues related to the acceptance of evidence in court [196], [197], [212]. Moreover, region-focused studies can be found in [213] and [197] for the United Kingdom and Australia, respectively.

TABLE 16. Qualitative analysis of the literature reviews related with digital forensic guidelines, frameworks, tools, and readiness. Notation: ✓ denotes that this topic is analysed, while ∘ denotes that its only partially discussed or just named.

		Qualitative topic discussion					
Reference	**Year**	Frameworks	Privacy/Ethics	Tools	Challenges	Suitability	Adaptability/Readiness
[176]	2018	✓	✓	✓	✓	✓	
[177]	2015	✓			∘		
[178]	2015				✓		✓
[196]	2018				✓		✓
[197]	2016	✓			✓	∘	
[175]	2020	✓			✓	✓	
[189]	2015				✓	∘	✓
[190]	2015				∘		✓
[193]	2016				✓		
[179]	2016	✓			✓	✓	
[195]	2018		✓		✓		✓
[180]	2017	✓		✓	∘		
[174]	2021				✓		
[15]	2021		✓	✓	✓		✓
[191]	2014		✓		✓		✓
[192]	2018			∘	✓		✓
[194]	2018				✓		∘

TABLE 17. Proposed representation of the content of a forensic report according to the inputs collected from the literature.

Step	Description	Technical level
1	Summary of contents	Low
2	Case information, description and examiners	Low
3	Forensic tools, versions, and main purpose of each tool. Limitations of each tool and scope.	Medium
4	Repository/evidence list and overview of the analysis and investigators behind such analysis.	Low
5	Summary of acquisition, seizure and analysis of evidence, and chain of custody preservation	Low
6	Technical aspects and methodology of the forensic analysis	High
7	Proof of replicability (repeated experiments led to same conclusions and are supported by data)	Medium
8	Link with other investigations, procedures and other remarks.	Medium

After analysing the previous literature of forensic reporting procedures and studying the technical level of the data to be included [214], [215], as well as analysing existing investigation models such as ISO/IEC 27043:2015 [216], we identified a set of key points and structural features that such document should include. In parallel, we analysed the technical level associated with each characteristic as reported in the literature and created a reporting guideline document, which is represented in Table 17. As it can be observed, summaries, overview descriptions and listings should be performed in a comprehensive, non-technical way. In the case of tool descriptions, as well as proofs guaranteeing the outcomes, the report should contain some technical yet understandable descriptions. Finally, the scientific aspects and details behind the analysis and the corresponding methodologies require descriptions that should be provided by qualified experts.

D. DATA MANAGEMENT AND ETHICS

When discussing digital forensics and respective technology readiness, the applicable regulatory frameworks should be considered as well. As seen in [195], integrating digital forensic readiness as a component in data protection legislation could improve actual practices across different sectors and countries.

In particular, this section highlights the regulatory requirements of working with data in Europe and in the European Union. To facilitate digital forensic readiness, tools should be developed and used in line with legal requirements, with special attention to the individual's privacy.

1) PRIVACY IN EUROPE

States have numerous responsibilities concerning the protection of their citizens. Although the protection of privacy (in its various forms) is important, it represents but one of the duties states should fulfil [217]. Other prominent duties relate to the need to protect the life and property of citizens, to prevent disorder, to ensure that justice occurs where individuals have been the victim of criminal activity and to protect national security both offline and online [218]. In modern western societies, it is often impossible to guarantee the exercise and protect such rights and in an absolute manner to all individuals all of the time due to competing interests of stakeholder groups. Respectively, privacy is only one of such values next to, e.g., security and the need for public order. To ensure security, the state likely has to take measures that may infringe upon the privacy of individuals [219]. This entails the acquisition of data or the conduct of surveillance to prevent *inter alia* acts of terrorism or crime. These activities clearly interfere with and limit the privacy of citizens but do so for desirable reasons. However, interference with such competing interests should be balanced, and the rights and freedoms of all groups in society should be respected to the greatest extent [217]. Respectively, the need to balance the privacy and security interests implies that security measures that infringe upon individual privacy are not acceptable unless they really are intended to meet a need that is relating to the protection the rights and interests of others. Where such

justification does not exist, infringement of individual privacy would not be acceptable.

2) DATA PROTECTION IN EUROPE

In consonance with the individual's data protection interest and society's own protective endeavours toward fighting crime and securing national security, the Council of Europe and European Union developed a common framework to be observed by technology developers, security agencies, including Police, and criminal justice system. The most relevant instruments of the Council of Europe relating to the processing of data as evidence are: 1) the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) in particular with reference to the protection of the rights to privacy and due process, 2) the Council of Europe Convention on Cybercrime, as this Convention remains the main and only international treaty which defines the substantive elements of cybercrimes [220], 3) the Council of Europe Convention on Mutual Assistance in Criminal Matters, and its 1978 Protocol [221], and 4) the Electronic Evidence Guide [222].

A second protocol concerning the ''Enhanced international cooperation on cybercrime and electronic evidence'' is also in development [223].

In European Union Art. 4 (2) of the Treaty on the European Union (TEU) states that national security is the sole responsibility of each Member State. To facilitate a harmonized approach to national security, the EU adopted several Directives and other legislative pieces in connection with criminal matters such as: 1) Charter of Fundamental Rights of the European Union, art 7 and 8. 2) 2016/679 General Data Protection Regulation 3) Statement of the Article 29 Working Party, Data protection and privacy aspects of cross-border access to electronic evidence, Brussels, 29 November 2017. 4) 2016/680/EU Law Enforcement Directive [224] 5) 2014/41/EU European Investigation Order Directive 6) EU 2000 Convention on mutual assistance in criminal matters 7) 910/2014 eIDAS Regulation [225] 8) Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders by ENISA, and 9) E-evidence package [226]

To rationalize the functioning and limit the increasing number of legal provisions, Regulation 2016/95 repealed certain acts in the field of police cooperation and judicial cooperation in criminal matters [227]. LEAs performing digital forensics have confidentiality case levels depending on the severity of the crime. The forensic examiners sign a special confidentiality agreement regarding data protection upon their employment. There are policies regarding data protection, all the case relevant data is kept only to the internal network, which is protected with the use of all the necessary measures (Secure Connections, encryption, controlled access at the physical location). The forensic examination equipment is not connected to the internet when examinations are conducted. The data in question in digital forensics is referred to as electronic evidence, defined as ''any information (comprising the output of analogue devices or data in digital format) of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device'' [228]. Respectively, to use such data, specific rules concerning the gathering and use of (digital) evidence should be adhered to as well. Electronic evidence is admissible in courts when the following sets of rules are adhered to: 1) general rules and principles concerning due process in criminal proceedings; 2) general rules of evidence in criminal proceedings and; 3) specific rules relating to electronic evidence in criminal proceedings [229].

There are both current, and to-be adopted elements of the applicable legal framework, but it must be underlined that as of now, there is no comprehensive international or European legal framework providing rules relating to evidence [230]. From these documents, five overarching principles can be deducted concerning the acquisition and use of electronic evidence. These are: data integrity, audit trail, specialist support, appropriate training, and legality [231]. National criminal procedure codes (referred above) contain further, specific provisions regarding the record and applicability of digital evidence in criminal procedures.

V. DISCUSSION

In Section III, we provided a topic-based taxonomy of the digital forensics literature. In what follows, we recall the challenges identified in each category and provide some strategies to overcome them.

A. THE ROAD AHEAD IN DIGITAL FORENSICS' TOPICS

After revising the challenges collected in cloud forensics, most of them are closely related to data management. More concretely, data acquisition, logging, limited access to forensic data, cross-border data access and exchange are vital parameters in cloud forensics. In terms of log management, Marty [232] proposed using log management architecture and the guidelines for application logging in SaaS service model using technologies such as Django, Javascript, Apache, and MySQL. A centralised logging scheme was proposed by Trenwith and Venter [233] to accelerate the investigation process and provide forensic readiness. Patrascu and Patriciu [234] proposed a scheme to monitor various parallel activities in a cloud environment. In addition to the previous works, several authors have devoted efforts towards efficient and secure evidence management in the cloud [235]–[237], including the use of blockchain such as seen in [238]. We believe that efficient evidence and logging collection mechanisms paired with secure and verifiable management of such evidence are crucial to guarantee sound cloud forensic investigations.

Network traffic forensics is a long-standing domain with numerous research efforts and tools. The main gaps that currently exist and on which future efforts shall be focused are related to the volume of the traffic, the different protocols that emerge mainly due to the IoT rise, and the fact that traffic is encrypted in most cases. As the use of computer systems and

the internet grows exponentially, the network traffic size to be analysed to conduct a forensics investigation rises. Methods that can efficiently analyse voluminous traces of network traffic are in high demand. Additionally, the heterogeneity of network traffic protocols increases the effort required to collect evidence from all available sources.

Last but not least, the main challenge that network forensics research faces nowadays is encrypted traffic. When digital forensic evidence acquisition happens at an intermediate node of the communication path, it is expected for the traffic payload to be encrypted, and methods capable of extracting information under such conditions are required.

Filesystems, Memory, and Data Storage forensics have attracted the research community's attention, as they are an abundant source of digital evidence. As discussed in Section III-E, the main challenge of these domains lies in the fact that there exist a large number of files and data contained in them. Thus, the efforts should focus on big data analysis and data mining techniques to extract the relevant investigation data from the vast amount of unrelated or redundant digital objects. Another issue is the case of distributed filesystem and databases or data stores, or when the forensic analysis should be conducted on the cloud. In the latter case, besides the specialised tools and methods, it also challenges collaboration and cooperation with the cloud service providers. Finally, most research works and tools are bound to specific system architecture, OS, or hardware implementation, so they have the drawback of becoming cumbersome to adjust existing solutions to new use cases and problems. In this context, more generic approaches that allow tool reuse in different cases are necessary.

The recovery of digital evidence from portable and/or mobile devices is the focus of mobile forensics (MF), a sub-branch of digital forensics. Seizure, acquisition, and examination/analysis are the three categories that mobile forensics processes fall into. Several challenges exist concerning mobile forensics, as presented in III-C. In the MF domain, the variety of embedded OSs with shorter product life cycles and the numerous smartphone manufacturers worldwide present significant challenges for applying sound forensics approaches. MF, in general, present a variety of challenges such as problems with data (anonymity-enforced browsing and other anonymity services, and the considerable volume of data acquired during an investigation), availability of forensic tools (MF research approaches have long focused on acquisition techniques, while minor importance was given to the other phases of MF investigative process) and security-oriented concerns (development of new and more sophisticated anti-forensic methods from mobile manufacturers). It is worth noting that MF is confronted with significant challenges regarding the overall MF processes' focus. For example, it is unclear whether investigation procedures should be model-specific for each device or generic enough to form a standardized set of forensics procedures guidelines. Another critical issue is the requirement to perform live forensics (mobile devices should be powered on). Finally, due to the security features built into modern mobile devices, an investigator must break into the device using an exploit that will almost certainly alter the data.

While the widespread adoption of IoT devices and IoT-related applications has improved data availability and operational excellence, it has also introduced new security and forensics challenges. As presented in Section III-D, several challenges exist concerning IoT forensics. Such challenges include managing multiple streams of data sources, the complicated three-tier architecture of IoT and the lack of standardized systems for capturing real-time logs and storing them in a valid uniform form. The preparation of highly detailed reports of all information gathered, its corresponding representation, and the lack of standardized systems for capturing real-time logs also serve as barriers to establishing sound IoT-related forensics mechanisms. Data encryption trends are also posing new challenges for IoT forensic investigators, and cryptographically protected storage systems are arguably one of the most significant roadblocks to effective digital forensic analysis. Interoperability and availability issues related to the vast number of connected IoT devices, the Big Data nature of IoT forensics evidence, and IoT forensics evidence's various security storage challenges also represent significant IoT-related forensics challenges. Finally, the IoT forensics domain faces several regulatory challenges, particularly those relating to data ownership in the cloud as defined by regional laws.

As seen in Section III-G, multimedia forensics is one of the most explored topics, according to the number of publications. Overall, while most authors focus on image forgery detection, anti-forensics is one of the most challenging problems. In this regard, more efforts should be devoted to counter anti-forensic mechanisms (i.e., as part of a global digital forensics concern) and methodologies to capture novel criminal trends with the help of sophisticated real-time object detection and classification systems. In addition, multi-layer systems and ontologies should be designed to cope with multiple threats at once, paired with the appropriate benchmarks to evaluate them. In parallel, the issues related to the vast amount of data to be processed should be minimised by proposing more efficient data storage and indexing mechanisms and introducing algorithms that can process, e.g., compressed data. Following such research paths and combining them with the proper legislation and standardisation mechanisms will improve the success of multimedia digital forensics investigations.

Blockchain forensics is a relatively new domain since blockchain technology accounts for a decade. In general, it has to be understood that the need for blockchain forensics methods is expected to grow in the coming years. As discussed in Section III-F current efforts focus on the examination of available data on public blockchain systems. One of the main challenges encountered is to provide efficient methods to conduct such analysis. The data on public ledgers continuously grows, while the storage structure differs amongst different implementations. Developing methods

and tools that can efficiently analyse data across commonly used blockchain platforms is required. Moreover, forensic analysis methods for blockchain systems' nodes will enable more thorough investigations with more detailed results for public and private blockchain systems. Finally, given the rising popularity of privacy enabled blockchain systems such as Monero or ZCash, additional effort will be required to support forensic investigations on cases that include interactions on such systems.

B. OPEN ISSUES AND FUTURE TRENDS

1) FORENSIC READINESS AND REPORTING

Given the continuous evolution of cybercrime and its harmful capacities, preventive strategies are paramount to fight criminal activities. The latter implies the need to reinforce digital forensic strategies at different levels, including guidelines, regulations, research and training to implement forensic readiness holistically. According to our literature analysis, one of the key points to reinforce the actual state of practice is the definition of interoperable and easy-to-adopt legislations since current ones cannot cope with the increasing sophistication and the ubiquitous nature of cybercrime. Therefore, it is crucial to devote efforts towards, e.g., interoperable cross-border models with their corresponding dissemination and training procedures, which all practitioners may adopt to accelerate investigations. It is also relevant to stress the necessity of appropriate forensic readability and reporting. First, effective communication between all the actors involved in a forensic investigation is essential to maximise the guarantees in court. Second, the proper documentation of investigations provides valuable feedback for future investigations, enhancing forensic readiness strategies. Third, the definition of a common reporting framework can accelerate investigations in which sometimes speed is crucial due to, e.g., the possible volatility of evidence or to reduce harm. To this end, we proposed a forensic reporting content representation by following the common denominators found in the literature in Section III. We argue that the devotion of more efforts on this final part of the forensic flow will enrich investigations with valuable feedback and successful prosecution guarantees.

2) FORENSIC PREPAREDNESS AND STANDARDS

While in Section IV we provided an overview of digital forensics standards, unfortunately, they do not suffice current needs. To name just two which are standing out on the tip of the iceberg, cloud and mobile related investigations need to have some standards on how to be performed. Addressing the need for mobile forensics, FORMOBILE[6] has initiated a broad dialogue and is developing a draft CENELEC Workshop Agreement to fill in this gap. However, due to the specificities of cloud, IoT, drones, etc., similar actions are expected in the near future.

Beyond standards and methods, there is a definite need from industry players, developers, system administrators etc., to foster a culture of *forensic preparedness*. Essentially, every organisation and resource provider must understand that its products and services are expected to suffer a successful cyber attack. Therefore, despite the countermeasures, recovery methods, and mitigation strategies, they need to implement policies and mechanisms to facilitate digital forensics. If the latter are not well-placed, while business continuity may not be severely harmed, one may not understand why and how the security event occurred, what needs to change, or miss even important evidence of the threat actor.

3) DECENTRALISATION AND IMMUTABILITY

The wide adoption of distributed platforms, e.g. blockchain solutions [80] and distributed storage and filesystems, imply significant challenges for digital forensics [239], [240]. Some of these structures have strong privacy guarantees and can be leveraged to exfiltrate data, orchestrate malicious campaigns [241]–[244], or siphon fraudulent payments [245]. Traditional logging mechanisms and access control systems allow an investigator to assess who, when, how or even from where are not relevant for many of these technologies. As a result, they are continuously abused by threat actors. These huge obstacles for digital forensics require further research on the field and the development of more targeted tools to extend the capabilities of digital investigators. In this regard, while the use of distributed platforms is not exempt from potential issues [240], they can also be potentially used to leverage community-based intelligence against threats and to leverage auditable forensic investigations [82], [246]–[248]. Following such an idea and in order to accelerate the response towards sophisticated threats and international campaigns, the community is devoting research efforts towards federated learning models [249], [250], and other emerging topics such as cognitive security [251], [252].

4) DATA PROTECTION AND ETHICS IN CRIMINAL INVESTIGATIONS

Ransomware may be regarded as the most obvious case of exploiting cryptographic primitives for malicious acts; nevertheless, this is not by any chance the only. Threat actors and cybercriminals, for instance, use encrypted and even covert channels to communicate, further hindering investigations. The latter has sparked a huge debates as many are promoting concepts such as *responsible encryption*[7] with the adoption of, e.g., weakened encryption, cryptographic schemes such as key escrow, backdooring of cryptographic primitives etc. [253]–[256]. While they may facilitate digital investigations, essentially, they undermine the scope of cryptography and security, opening the door for many interpretations on what lawful interception is, when it can be performed, by whom, let alone the exploitation of the mechanisms by already malicious actors as the backdoor would be already implanted. The debate is undergoing and spans

[6] https://formobile-project.eu/

[7] https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval

multiple sectors beyond digital forensics. While fostering such approaches may greatly benefit digital forensics, the ethical and legal implications hinder such adoption and are received by the security community with scepticism. As discussed, anti-forensics methods are a challenge for almost all domains of digital forensics. Nevertheless, with the growing adoption of TPM and TEE, these challenges can be significantly augmented. For instance, as illustrated by Dunn *et al.* [257] ransomware can exploit these technologies to render decryption key extraction impossible. Nevertheless, it is clear that these technologies introduce significant challenges for digital investigators since they may deprive them of access to critical information. In this regard, it is essential to study methods for, e.g. live forensics in the presence of TPM and TEE and to explore how the missing information can be compensated.

5) AUTOMATION AND EXPLAINABILITY

The continuous increase in reported cybercrimes apart from the impact on the victims implies a lot of effort from investigators to analyse the cases. Therefore, automation of digital forensics inevitably becomes a need. While automated methods for collecting log files and algorithms to identify anomalies or even correlating some events may exist, this does not practically translate to automated digital forensics. Even if one does not consider APT attacks, one must understand that each case has particularities differentiating it from the others. Moreover, a digital investigator has to fill in the gaps of missing information that the attacker managed to cover, including those that security mechanisms failed to record or those erroneously reported. The above implies the development of advanced machine learning and AI algorithms and tools that will underpin future digital forensics investigations. An important part of these systems is undoubtedly understanding the scope of the investigation and the explainability of the results [258], which is critical to assess the impact of current investigations and quantify their effectiveness [14], a critical step to ensure the implementation of the proper measures. The latter is a crucial part of AI and machine learning modules that have to be introduced as in order for a piece of evidence to be admissible in a court of law, one has to justify not only how and from where it has been collected but to also prove the relevance to the case, how it was used, and why it is linked with the rest of the evidence. In essence, future digital forensics systems would have to argue and reason on the collected information in a human-readable manner. The latter is a huge step forward compared to the existing state where systems prioritise log events and present the analysts with known malicious patterns in the logs, malicious binaries, or connections that deviate specific norms.

6) FORENSIC GUIDELINES AND BEST PRACTICES

One of the main strategies to reduce the impact of cybercrime is to implement the recommendations of the security guidelines and directives developed by agencies such as ENISA and NIST. The current threat landscape [6], which includes ransomware, malware, and threats against data availability and veracity, affect digital forensics in different dimensions, regardless of the topic. NIST recently published a state of the art analysis of cloud-related challenges [34], which is aligned with the claims collected by in the cloud-based digital forensics literature reviews state in Section III-A. In the case of networks, ENISA elaborated an extensive set of security objectives and discussed them along with their corresponding recommendation measures in the topics of electronic communications [259] as well as 5G networks [260]. NIST provides security guidelines for managing mobile devices in their draft SP 800-124 (rev2) [261]. The recommendations include scenarios from organization-provided to personally-owned devices and describes technologies and strategies that can be used as countermeasures and mitigations. In the context of IoT, NIST released a set of documents related to IoT device cybersecurity, covering aspects from the design and manufacturing of the components to their disposal [262]. In parallel, ENISA also proposed a comprehensive set of security guidelines targeting all the entities involved in the supply chain of IoT to improve security decisions when designing, building, deploying, and assessing IoT technologies [263]. Concerning data storage and data processing, several guidelines have been proposed during the past years to reduce data breaches [264], and the proper deployment of data storage mechanisms that enable privacy by design [265]–[267], and forensic readiness [268]. Finally, despite the existence of such guidelines, forensic frameworks accommodating procedures adapted to novel types of cybercrime such as in e.g. social networks [269], and the proper review and evaluation of an investigation process, are necessary to assess the quality of forensic investigations [270].

VI. CONCLUSION AND FINAL REMARKS

The digitisation of our daily lives is a double-edged sword as beyond the myriad of advantages and comforts it provides, it introduces security and privacy issues. Motivated by the lack of a general view of the digital forensics ecosystem, mainly because different topics are explored in an isolated way and aiming to answer several research questions/concerns, this manuscript seeks to fill a literature gap by proposing a review of reviews in the field of digital forensics. Following a thorough research methodology, we identified the main digital forensics topics. We performed a taxonomy by documenting the current state of the art and practice and the main challenges in each of them. Moreover, we analysed these challenges with a cross-domain perspective to highlight their relevance according to the times they were discussed in the literature. According to the outcomes (i.e. see Section III-I), such analysis provided us with enough evidence to prove that the digital forensics community could benefit from closer collaborations and cross-topic research since it appears that researchers are trying to find solutions to the same problems in parallel, sometimes without noticing it.

By merging the information of Table 10 and Figure 4, we extracted the amount of cross-domain challenges that

each topic has in each forensic phase, and reported them in Table 18. As it can be observed, data acquisition along with investigation and forensic analysis are the phases that entail more challenges, according to the research community. If we analyse the data at a topic level, we can observe that IoT has many challenges to overcome in such phases. The same applies to Multimedia and Mobile forensics. Since we focus on the extracted challenges as collected in our literature review, the fact that some challenges have not been highlighted either at topic or forensic phase level may indicate that researchers and practitioners have not devoted enough effort to them, or perhaps highlights lack of discussion towards them. Such interesting domains include value chain and financial forensics. Like other domains, the business sector's ongoing digitisation means that sound value chain forensics mechanisms will be almost necessary within any corporate strategy for the years to come. Therefore, the potentially unexplored issues in such cases require proactive initiatives before they become obstacles in the near future.

TABLE 18. Limitations per topic according to each phase as depicted in Figure 4.

	Standards & legislation	Data acquisition & pre-processing	Investigation & forensic analysis	Reporting & presentation
Cloud	2	3	2	1
Networks		2	1	
Mobile	2	3	3	
IoT	2	4	5	1
FS & DB	1	3	2	1
Blockchain		2	1	
Multimedia		4	3	

Further to merely listing the state of practice and proposing research directions according to the identified challenges, we analysed crucial aspects of digital forensics such as standards, forensic readiness, forensic reporting, and discussed the ethical and legal aspects of data management in Europe in Section IV. The insights gathered from such analysis, which were represented in the form of structured tables, qualitative literature analysis, and a proposed representation of forensic report content, successfully answered the research questions presented in Table 1.

Finally, we discussed the main takeaways of this article and showcased several challenges that the digital forensics community will face in the upcoming years in Section V. In this regard, we proposed some ideas to prevent and/or overcome them while recalling the need to design efficient and cross-domain strategies since the latter will guarantee faster and more robust outcomes, hopefully minimising the impact of criminal activities.

Notably, some limitations of our approach are worth mentioning. Since our article is a review of reviews, we may have missed some recent advances and challenges should these have not yet been collected in recent surveys. Moreover, we only considered peer-reviewed journals, which may have lessened our approach's comprehensive and interdisciplinary nature. However, we opted for this methodology since usually, literature reviews are mature and long term works not likely to be published in conferences as they do not require a fast positioning. By discussing the open issues and future trends in digital forensics, and after observing that many of the challenges raised years ago are still not solved, we believe that our literature analysis reflects with high fidelity the current state of practice and the potential challenges that may arise in the years to come, providing a fruitful ground of research.

The inherent cross-jurisdiction nature of modern cybercrime paired with the abuse of cutting edge technologies mandates more coordinated efforts from the security and research community. With the continuously increasing amount of data that have to be analysed, it is straightforward that manual analysis is almost at its limits. The use of fine-grained IoCs may significantly reduce the effort of the investigator. However, as already discussed, this is not always possible, especially when non-traditional computing devices are used, e.g. IoT, mobile, cloud. As a result, machine learning and artificial intelligence are gradually being integrated into the logic of many tools and methods. Nevertheless, the reasoning of the results in an understandable human manner is a cross-domain challenge. Moreover, the standardisation of digital forensics processes for cloud, mobile, IoT, drones, etc., is becoming a high priority since they are an indispensable part of almost all modern digital investigations. Finally, the consensus on developing these standards and the coordinated efforts made over the past few years for countering cybercrime must be leveraged to homogenise the legislation across jurisdictions and facilitate digital investigations. A common answer to the problem and using the same measures would create a strong response against cybercrime and improve response time to security incidents and their analysis.

ACKNOWLEDGMENT

The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

REFERENCES

[1] J. I. Thornton and J. Peterson, "The general assumptions and rationale of forensic identification," *Modern scientific evidence: Law Sci. expert testimony*, vol. 2, p. 13, 1997.

[2] E. Locard, *Manuel de Technique Policière: Les Constats, les Empreintes Digitales*, 2nd ed. Paris, France: Payot, 1934.

[3] F. L. Wellman and H. Münsterberg, "The art of cross-examination," *Amer. Bar Assoc. J.*, vol. 10, no. 4, p. 249, 1924. [Online]. Available: http://www.jstor.org/stable/25711556

[4] M. Pollitt, "A history of digital forensics," in *IFIP International Conference on Digital Forensics*. Berlin, Germany: Springer, 2010, pp. 3–15.

[5] (2019). I. G. C. for Innovation. *Global Guidelines for Digital Forensics Laboratories*. [Online]. Available: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_Globa%lGuidelinesDigitalForensicsLaboratory.pdf

[6] (2021). The European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2021*. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[7] P. Purnaye and V. Kulkarni, "A comprehensive study of cloud forensics," *Arch. Comput. Methods Eng.*, vol. 29, no. 1, pp. 1–14, 2021.

[8] C. Pasquini, I. Amerini, and G. Boato, "Media forensics on social media platforms: A survey," *EURASIP J. Inf. Secur.*, vol. 2021, no. 1, pp. 1–19, Dec. 2021.

[9] K. Nance, H. Armstrong, and C. Armstrong, "Digital forensics: Defining an education agenda," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, 2010, pp. 1–10.

[10] A. M. Marshall, "Quality standards and regulation: Challenges for digital forensics," *Meas. Control*, vol. 43, no. 8, pp. 243–247, Oct. 2010.

[11] P. S. Chen, L. M. Tsai, Y.-C. Chen, and G. Yee, "Standardizing the construction of a digital forensics laboratory," in *Proc. 1st Int. Workshop Systematic Approaches Digit. Forensic Eng. (SADFE)*, Nov. 2005, pp. 40–47.

[12] A. Varol and Y. U. Sönmez, "Review of evidence collection and protection phases in digital forensics process," *Int. J. Inf. Secur. Sci.*, vol. 6, no. 4, pp. 39–46, 2017.

[13] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in hyperledger composer," *Digit. Invest.*, vol. 28, pp. 44–55, Mar. 2019.

[14] R. E. Overill and J. Collie, "Quantitative evaluation of the results of digital forensic investigations: A review of progress," *Forensic Sci. Res.*, vol. 6, no. 1, pp. 13–18, Jan. 2021.

[15] K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102237.

[16] M. Fire and C. Guestrin, "Over-optimization of academic publishing metrics: Observing Goodhart's law in action," *GigaScience*, vol. 8, no. 6, Jun. 2019.

[17] H. Hunt, A. Pollock, P. Campbell, L. Estcourt, and G. Brunton, "An introduction to overviews of reviews: Planning a relevant research question and objective for an overview," *Systematic Rev.*, vol. 7, no. 1, pp. 1–9, Dec. 2018.

[18] J. E. McKenzie and S. E. Brennan, "Overviews of systematic reviews: Great promise, greater challenge," *Systematic Rev.*, vol. 6, no. 1, pp. 1–4, Dec. 2017.

[19] E. Aromataris, R. Fernandez, C. M. Godfrey, C. Holly, H. Khalil, and P. Tungpunkom, "Summarizing systematic reviews: Methodological development, conduct and reporting of an umbrella review approach," *Int. J. Evidence Based Healthcare*, vol. 13, no. 3, pp. 132–140, 2015.

[20] M. Pollock, R. M. Fernandes, D. Pieper, A. C. Tricco, M. Gates, A. Gates, and L. Hartling, "Preferred reporting items for overviews of reviews (PRIOR): A protocol for development of a reporting guideline for overviews of reviews of healthcare interventions," *Systematic Rev.*, vol. 8, no. 1, pp. 1–9, Dec. 2019.

[21] D. Denyer and D. Tranfield, "Producing a systematic review," in *The Sage Handbook of Organizational Research Methods*. Los Angeles, CA, USA: SAGE, 2009, pp. 671–689.

[22] R. Pranckutė, "Web of science (WoS) and scopus: The titans of bibliographic information in Today's academic world," *Publications*, vol. 9, no. 1, p. 12, Mar. 2021.

[23] J. vom Brocke, A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, and A. Cleven, "Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research," *Commun. Assoc. Inf. Syst.*, vol. 37, no. 1, p. 9, 2015.

[24] M. E. Alex and R. Kishore, "Forensics framework for cloud computing," *Comput. Elect. Eng.*, vol. 60, pp. 193–205, May 2017.

[25] M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 8, pp. 610–629, 2019.

[26] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digit. Invest.*, vol. 13, pp. 38–57, Jun. 2015.

[27] G. Palmer *et al.*, "A road map for digital forensic research," in *Proc. 1st Digit. Forensic Res. Workshop*, New York, NY, USA, 2001, pp. 27–30.

[28] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," *Digit. Invest.*, vol. 10, no. 1, pp. 34–43, 2013.

[29] S. Park, Y. Kim, G. Park, O. Na, and H. Chang, "Research on digital forensic readiness design in a cloud computing-based smart work environment," *Sustainability*, vol. 10, no. 4, p. 1203, Apr. 2018.

[30] S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, "A survey on cloud forensics challenges and solutions," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 6285–6314, Dec. 2016.

[31] A. Aminnezhad, A. Dehghantanha, M. T. Abdullah, and M. Damshenas, "Cloud forensics issues and opportunities," *Int. J. Inf. Process. Manage.*, vol. 4, no. 4, pp. 76–85, Jun. 2013.

[32] N. H. A. Rahman, and K.-K. R. Choo, "A survey of information security incident handling in the cloud," *Comput. Secur.*, vol. 49, pp. 45–69, Mar. 2015.

[33] B. Manral, G. Somani, K.-K.-R. Choo, M. Conti, and M. S. Gaur, "A systematic survey on cloud forensics challenges, solutions, and future directions," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–38, Nov. 2020.

[34] N. I. of Standards and Technology. (2020). *Nistir 8006 NIST Cloud Computing Forensic Science Challenges*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf

[35] A. Alenezi, H. F. Atlam, and G. B. Wills, "Experts reviews of a cloud forensic readiness framework for organizations," *J. Cloud Comput.*, vol. 8, no. 1, Dec. 2019.

[36] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digit. Invest.*, vol. 7, nos. 1–2, pp. 14–27, Oct. 2010.

[37] (2020). N. T. S. Coalition. *Cybersecurity Report 2020*. [Online]. Available: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

[38] C. Patsakis, F. Casino, N. Lykousas, and V. Katos, "Unravelling Ariadne's thread: Exploring the threats of decentralised DNS," *IEEE Access*, vol. 8, pp. 118559–118571, 2020.

[39] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," *J. Netw. Comput. Appl.*, vol. 40, pp. 307–324, Apr. 2014.

[40] S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, and I. Ahmad, "Network forensics: Review, taxonomy, and open challenges," *J. Netw. Comput. Appl.*, vol. 66, pp. 214–235, May 2016.

[41] A. Nisioti, A. Mylonas, P. D. Yoo, and V. Katos, "From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3369–3388, 4th Quart., 2018.

[42] F. Sharevski, "Towards 5G cellular network forensics," *EURASIP J. Inf. Secur.*, vol. 2018, no. 1, p. 8, Dec. 2018.

[43] D. Takahashi, Y. Xiao, Y. Zhang, P. Chatzimisios, and H.-H. Chen, "IEEE 802.11 user fingerprinting and its applications for intrusion detection," *Comput. Math. Appl.*, vol. 60, no. 2, pp. 307–318, Jul. 2010.

[44] L. F. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Forensic Sci. Int., Digit. Invest.*, vol. 32, Mar. 2020, Art. no. 200892.

[45] I. R. Adeyemi, S. A. Razak, and N. A. N. Azhan, "A review of current research in network forensic analysis," *Int. J. Digit. Crime Forensics*, vol. 5, no. 1, pp. 1–26, Jan. 2013.

[46] A. A. Ahmed and N. A. K. Zaman, "Attack intention recognition: A review," *IJ Netw. Secur.*, vol. 19, no. 2, pp. 244–250, 2017.

[47] H.-C. Chu, D.-J. Deng, and H.-C. Chao, "Potential cyberterrorism via a multimedia smart phone based on a Web 2.0 application via ubiquitous Wi-Fi access points and the corresponding digital forensics," *Multimedia Syst.*, vol. 17, no. 4, pp. 341–349, Jul. 2011.

[48] K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, "Current and future trends in mobile device forensics: A survey," *ACM Comput. Surv.*, vol. 51, no. 3, pp. 1–31, 2018.

[49] A. Farjamfar, M. T. Abdullah, R. Mahmod, and N. Izura Udzir, "A review on mobile device's digital forensic process models," *Res. J. Appl. Sci., Eng. Technol.*, vol. 8, no. 3, pp. 358–366, Jul. 2014.

[50] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, "A critical review of 7 years of mobile device forensics," *Digit. Invest.*, vol. 10, no. 4, pp. 323–349, Dec. 2013.

[51] X. Wan, J. He, G. Liu, N. Huang, X. Zhu, B. Zhao, and Y. Mai, "Survey of digital forensics technologies and tools for Android based intelligent devices," *Int. J. Digit. Crime Forensics*, vol. 7, no. 1, pp. 1–25, Jan. 2015.

[52] J. Hou, Y. Li, J. Yu, and W. Shi, "A survey on digital forensics in Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 1–15, Jan. 2020.

[53] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[54] R. Kamal, E. E.-D. Hemdan, and N. El-Fishway, "A review study on blockchain-based iot security and forensics," *Multimedia Tools Appl.*, vol. 80, pp. 1–32, Sep. 2021.

[55] H. F. Atlam, E. El-Din Hemdan, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Internet of Things forensics: A review," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100220.

[56] P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama, and B. B. Bastaki, "The complexity of Internet of Things forensics: A state-of-the-art review," *Forensic Sci. Int., Digit. Invest.*, vol. 38, Sep. 2021, Art. no. 301210.
[57] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics," *Digit. Invest.*, vol. 29, pp. 43–54, Jun. 2019.
[58] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, W. H. Alshoura, and H. Arshad, "The Internet of Things security: A survey encompassing unexplored areas and new insights," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102494.
[59] O. Yakubu, N. C. Babu, and O. Adjei, "A review of digital forensic challenges in the Internet of Things (IoT)," *Int. J. Mech. Eng. Technol.*, vol. 9, no. 1, pp. 915–923, 2018.
[60] N. Koroniotis, N. Moustafa, and E. Sitnikova, "Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions," *IEEE Access*, vol. 7, pp. 61764–61785, 2019.
[61] A. Ross, S. Banerjee, and A. Chowdhury, "Security in smart cities: A brief review of digital forensic schemes for biometric data," *Pattern Recognit. Lett.*, vol. 138, pp. 346–354, Oct. 2020.
[62] H. Studiawan, F. Sohel, and C. Payne, "A survey on forensic investigation of operating system logs," *Digit. Invest.*, vol. 29, pp. 1–20, Jun. 2019.
[63] S. Khan, A. Gani, A. W. A. Wahab, M. A. Bagiwa, M. Shiraz, S. U. Khan, R. Buyya, and A. Y. Zomaya, "Cloud log forensics: Foundations, state of the art, and future directions," *ACM Comput. Surveys*, vol. 49, no. 1, pp. 1–42, Mar. 2017.
[64] R. A. Awad, S. Beztchi, J. M. Smith, B. Lyles, and S. Prowell, "Tools, techniques, and methodologies: A survey of digital forensics for scada systems," in *Proc. 4th Annu. Ind. Control Syst. Secur. Workshop*, 2018, pp. 1–8.
[65] M. Botacin, P. L. D. Geus, and A. Grégio, "Who watches the watchmen: A security-focused review on current state-of-the-art techniques, tools, and methods for systems and binary analysis on modern platforms," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–34, Jul. 2019.
[66] T. Latzo, R. Palutke, and F. Freiling, "A universal taxonomy and survey of forensic memory acquisition techniques," *Digit. Invest.*, vol. 28, pp. 56–69, Mar. 2019.
[67] G. Osbourne, "Memory forensics: Review of acquisition and analysis techniques," Defence Sci. Technol. Organisation Edinburgh (Australia) Cyber Electron. Warfare Div, Tech. Rep., 2013.
[68] A. Case and G. G. Richard, "Memory forensics: The path forward," *Digit. Invest.*, vol. 20, pp. 23–33, Mar. 2017.
[69] A. Al-Dhaqm, S. A. Razak, D. A. Dampier, K.-K. R. Choo, K. Siddique, R. A. Ikuesan, A. Alqarni, and V. R. Kebande, "Categorization and organization of database forensic investigation processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020.
[70] O. M. Adedayo and M. S. Olivier, "Ideal log setting for database forensics reconstruction," *Digit. Invest.*, vol. 12, pp. 27–40, Mar. 2015.
[71] R. Chopade and V. K. Pachghare, "Ten years of critical review on database forensics research," *Digit. Invest.*, vol. 29, pp. 180–197, Jun. 2019.
[72] W. K. Hauger and M. S. Olivier, "NOSQL databases: Forensic attribution implications," *SAIEE Afr. Res. J.*, vol. 109, no. 2, pp. 119–132, Jun. 2018.
[73] V. Jusas, D. Birvinskas, and E. Gahramanov, "Methods and tools of digital triage in forensic context: Survey and future directions," *Symmetry*, vol. 9, no. 4, p. 49, Mar. 2017.
[74] A. Al-Dhaqm, S. Razak, R. A. Ikuesan, V. R. Kebande, and S. Hajar Othman, "Face validation of database forensic investigation metamodel," *Infrastructures*, vol. 6, no. 2, p. 13, Jan. 2021.
[75] I. Sutherland, J. Evans, T. Tryfonas, and A. J. C. Blyth "Acquiring volatile operating system data tools and techniques," *Operating Syst. Rev.*, vol. 42, pp. 65–73, Apr. 2008.
[76] N. Beebe and J. Clark, "Dealing with terabyte data sets in digital investigations," in *Proc. IFIP Int. Fed. Inf. Process.*, vol. 194, 2006, pp. 3–16.
[77] D. Quick and K.-K.-R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," *Digit. Invest.*, vol. 11, no. 4, pp. 273–294, Dec. 2014.
[78] B. Almaslukh, "Forensic analysis using text clustering in the age of large volume data: A review," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 6, pp. 71–76, 2019.
[79] V. H. G. Moia and M. A. A. Henriques, "Similarity digest search: A survey and comparative analysis of strategies to perform known file filtering using approximate matching," *Secur. Commun. Netw.*, vol. 2017, pp. 1–17, 2017.
[80] F. Casino, T. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Inform.*, vol. 36, pp. 55–81, Mar. 2019.
[81] B. Shanmugam, S. Azam, K. C. Yeo, J. Jose, and K. Kannoorpatti, "A critical review of bitcoins usage by cybercriminals," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2017, pp. 1–7.
[82] T. K. Dasaklis, F. Casino, and C. Patsakis, "Sok: Blockchain solutions for forensics," in *Technology Development for Security Practitioners*. Cham, Switzerland: Springer, 2021.
[83] A. Balaskas and V. N. L. Franqueira, "Analytical tools for blockchain: Review, taxonomy and open challenges," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services (Cyber Security)*, Jun. 2018, pp. 1–8.
[84] A. Turner and A. S. M. Irwin, "Bitcoin transactions: A digital discovery of illicit activity on the blockchain," *J. Financial Crime*, vol. 25, no. 1, pp. 109–130, Jan. 2018.
[85] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Comput. Surv.*, vol. 53, no. 3, pp. 1–43, May 2021.
[86] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 341–390, 1st Quart., 2021.
[87] Z. Wang, H. Jin, W. Dai, K.-K.-R. Choo, and D. Zou, "Ethereum smart contract security research: Survey and future research opportunities," *Frontiers Comput. Sci.*, vol. 15, no. 2, Apr. 2021, Art. no. 152802.
[88] W. Koerhuis, T. Kechadi, and N.-A. Le-Khac, "Forensic analysis of privacy-oriented cryptocurrencies," *Forensic Sci. Int., Digit. Invest.*, vol. 33, Jun. 2020, Art. no. 200891.
[89] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, 3rd Quart., 2020.
[90] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, "A survey on long-range attacks for proof of stake protocols," *IEEE Access*, vol. 7, pp. 28712–28725, 2019.
[91] H. Farid, "Image forgery detection," *IEEE Signal Process. Mag.*, vol. 26, no. 2, pp. 16–25, Mar. 2009.
[92] K. A. P. da Costa, J. P. Papa, L. A. Passos, D. Colombo, J. D. Ser, K. Muhammad, and V. H. C. de Albuquerque, "A critical literature survey and prospects on tampering and anomaly detection in image data," *Appl. Soft Comput.*, vol. 97, Dec. 2020, Art. no. 106727.
[93] A. H. Saber, M. A. Khan, and B. G. Mejbel, "A survey on image forgery detection using different forensic approaches," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 5, no. 3, pp. 361–370, 2020.
[94] L. Zheng, Y. Zhang, and L. Vrizlynn, "A survey on image tampering and its detection in real-world photos," *J. Vis. Commun. Image Represent.*, vol. 58, pp. 380–399, Jan. 2019.
[95] S. Bourouis, R. Alroobaea, A. Alharbi, M. Andejany, and S. Rubaiee, "Recent advances in digital multimedia tampering detection for forensics analysis," *Symmetry*, vol. 12, no. 11, pp. 1–26, 2020.
[96] H. Kaur and N. Jindal, "Image and video forensics: A critical survey," *Wireless Pers. Commun.*, vol. 112, no. 2, pp. 1281–1302, May 2020.
[97] M. D. Ansari, E. Rashid, S. Skandha, and S. K. Gupta, "A comprehensive analysis of image forensics techniques: Challenges and future direction," *Recent Patents Eng.*, vol. 13, pp. 1–10, Dec. 2019.
[98] R. C. Pandey, S. K. Singh, and K. K. Shukla, "Passive forensics in image and video using noise features: A review," *Digit. Invest.*, vol. 19, pp. 1–28, Dec. 2016.
[99] S. Gupta, N. Mohan, and P. Kaushal, "Passive image forensics using universal techniques: A review," *Artif. Intell. Rev.*, vol. 2021, pp. 1–51, Jul. 2021.
[100] M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," *Signal Process., Image Commun.*, vol. 39, pp. 46–74, Nov. 2015.
[101] A. R. Abrahim, M. S. M. Rahim, and G. B. Sulong, "Literature review: Detection of image splicing forgery," *Int. J. Appl. Eng. Res.*, vol. 12, no. 22, pp. 11855–11861, 2017.
[102] R. Dixit and R. Naskar, "Review, analysis and parameterisation of techniques for copy–move forgery detection in digital images," *IET Image Process.*, vol. 11, no. 9, pp. 746–759, Sep. 2017.
[103] S. Teerakanok and T. Uehara, "Copy-move forgery detection: A state-of-the-art technical review and analysis," *IEEE Access*, vol. 7, pp. 40550–40568, 2019.

[104] Z. Zhang, C. Wang, and X. Zhou, "A survey on passive image copy-move forgery detection," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 6–31, 2018.
[105] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digital Invest.*, vol. 10, no. 3, pp. 226–245, Oct. 2013.
[106] R. R. Ali, K. M. Mohamad, S. Jamel, and S. K. A. Khalid, "A review of digital forensics methods for JPEG file carving," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 17, pp. 5841–5856, 2018.
[107] M. J. Khan, H. S. Khan, A. Yousaf, K. Khurshid, and A. Abbas, "Modern trends in hyperspectral image analysis: A review," *IEEE Access*, vol. 6, pp. 14118–14129, 2018.
[108] P. Korus, "Digital image integrity—A survey of protection and verification techniques," *Digit. Signal Process.*, vol. 71, pp. 1–26, Dec. 2017.
[109] T. Julliand, V. Nozick, and H. Talbot, "Image noise and digital image forensics," in *Proc. Int. Workshop Digit. Watermarking*. Cham, Switzerland: Springer, 2015, pp. 3–17.
[110] S. Chutani and A. Goyal, "A review of forensic approaches to digital image steganalysis," *Multimedia Tools Appl.*, vol. 78, no. 13, pp. 18169–18204, Jul. 2019.
[111] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *J. Inf. Secur. Appl.*, vol. 40, pp. 217–235, Jun. 2018.
[112] X. Luo, F. Liu, S. Lian, C. Yang, and S. Gritzalis, "On the typical statistic features for image blind steganalysis," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1404–1422, Aug. 2011.
[113] P. Yang, D. Baracchi, R. Ni, Y. Zhao, F. Argenti, and A. Piva, "A survey of deep learning-based source image forensics," *J. Imag.*, vol. 6, no. 3, p. 9, Mar. 2020.
[114] M. Dalal and M. Juneja, "Steganography and steganalysis (in digital forensics): A cybersecurity guide," *Multimedia Tools Appl.*, vol. 80, no. 4, pp. 5723–5771, Feb. 2021.
[115] V. N. L. Franqueira, J. Bryce, N. Al Mutawa, and A. Marrington, "Investigation of indecent images of children cases: Challenges and suggestions collected from the trenches," *Digit. Invest.*, vol. 24, pp. 95–105, Mar. 2018.
[116] L. Sanchez, C. Grajeda, I. Baggili, and C. Hall, "A practitioner survey exploring the value of forensic tools, AI, filtering, & safer presentation for investigating child sexual abuse material (CSAM)," *Digit. Invest.*, vol. 29, pp. S124–S142, Jul. 2019.
[117] J. Cifuentes, A. L. S. Orozco, and L. J. G. Villalba, "A survey of artificial intelligence strategies for automatic detection of sexually explicit videos," *Multimedia Tools Appl.*, vol. 39, pp. 1–18, Nov. 2021.
[118] K. V. Açar, "Osint by crowdsourcing: A theoretical model for online child abuse investigations," *Int. J. Cyber Criminol.*, vol. 12, no. 1, pp. 206–229, 2018.
[119] E. Nowroozi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A survey of machine learning techniques in adversarial image forensics," *Comput. Secur.*, vol. 100, Jan. 2021, Art. no. 102092.
[120] M. Dalal and M. Juneja, "Video steganalysis to obstruct criminal activities for digital forensics: A survey," *Int. J. Electron. Secur. Digit. Forensics*, vol. 10, no. 4, pp. 338–355, 2018.
[121] S. Kingra, N. Aggarwal, and R. D. Singh, "Video inter-frame forgery detection: A survey," *Indian J. Sci. Technol.*, vol. 9, no. 44, Nov. 2016.
[122] N. A. Shelke and S. S. Kasana, "A comprehensive survey on passive techniques for digital video forgery detection," *Multimedia Tools Appl.*, vol. 80, no. 4, pp. 6247–6310, Feb. 2021.
[123] A. S. Shahraki, H. Sayyadi, M. H. Amri, and M. Nikmaram, "Survey: Video forensic tools," *J. Theor. Appl. Inf. Technol.*, vol. 47, no. 1, pp. 98–107, 2013.
[124] M. Alsmirat, R. Al-Hussien, W. Al-Sarayrah, Y. Jararweh, and M. Etier, "Digital video forensics: A comprehensive survey," *Int. J. Adv. Intell. Paradigms*, vol. 15, no. 4, pp. 437–456, 2020.
[125] F. Becerra-Riera, A. Morales-González, and H. Méndez-Vázquez, "A survey on facial soft biometrics for video surveillance and forensic applications," *Artif. Intell. Rev.*, vol. 52, no. 2, pp. 1155–1187, Aug. 2019.
[126] S. T and S. M. Thampi, "Nighttime visual refinement techniques for surveillance video: A review," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 32137–32158, Nov. 2019.
[127] R. D. Singh and N. Aggarwal, "Video content authentication techniques: A comprehensive survey," *Multimedia Syst.*, vol. 24, no. 11, pp. 211–240, Mar. 2018.
[128] M. Zakariah, M. K. Khan, and H. Malik, "Digital multimedia audio forensics: Past, present and future," *Multimedia Tools Appl.*, vol. 77, no. 1, pp. 1009–1040, Jan. 2018.
[129] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy," *Digit. Invest.*, vol. 18, pp. S66–S75, Aug. 2016.
[130] M. A. Qureshi and E. M. El-Alfy, "Bibliography of digital image anti-forensics and anti-anti-forensics techniques," *IET Image Process.*, vol. 13, no. 11, pp. 1811–1823, Sep. 2019.
[131] F. Guibernau, "Catch me if you can!—Detecting sandbox evasion techniques," in *Proc. USENIX Assoc.*, San Francisco, CA, USA, Jan. 2020.
[132] P. Chen, C. Huygens, L. Desmet, and W. Joosen, "Advanced or not? A comparative study of the use of anti-debugging and anti-VM techniques in generic and targeted malware," in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*. Cham, Switzerland: Springer, 2016, pp. 323–336.
[133] A. Bulazel and B. Yener, "A survey on automated dynamic malware analysis evasion and counter-evasion: PC, mobile, and Web," in *Proc. 1st Reversing Offensive-oriented Trends Symp. (ROOTS)*, 2017, pp. 1–21.
[134] R. R. Branco, G. N. Barbosa, and P. D. Neto, "Scientific but not academical overview of malware anti-debugging, anti-disassembly and anti-VM technologies," *Black Hat*, vol. 1, pp. 1–27, Jul. 2012.
[135] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," *Digit. Invest.*, vol. 3, pp. 44–49, Sep. 2006.
[136] S. Alharbi, J. Weber-Jahnke, and I. Traore, "The proactive and reactive digital forensics investigation process: A systematic literature review," in *Information Security and Assurance*, T.-H. Kim, H. Adeli, R. J. Robles, and M. Balitanas, Eds. Berlin, Heidelberg: Springer, 2011, pp. 87–100.
[137] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghaban, "Research challenges and opportunities in drone forensics models," *Electronics*, vol. 10, no. 13, p. 1519, Jun. 2021.
[138] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," *Digit. Invest.*, vol. 16, pp. 1–11, Mar. 2016.
[139] S. Atkinson, G. Carr, C. Shaw, and S. Zargari, *Drone Forensics: The Impact and Challenges*. Cham, Switzerland: Springer, 2021, pp. 65–124.
[140] F. Adelstein, "Live forensics: Diagnosing your system without killing it first," *Commun. ACM*, vol. 49, no. 2, pp. 63–66, Feb. 2006.
[141] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/drone) forensic framework," *Digit. Invest.*, vol. 30, pp. 52–72, Sep. 2019.
[142] E. Mantas and C. Patsakis, "Who watches the new watchmen? The challenges for drone digital forensics investigations," *arXiv preprint arXiv:2021.12640*, 2021.
[143] M. Keyvanpour, M. Moradi, and F. Hasanzadeh, "Digital forensics 2.0," in *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*. Cham, Switzerland: Springer, 2014, pp. 17–46.
[144] T. Sangkaran, A. Abdullah, and N. Z. JhanJhi, "Criminal network community detection using graphical analytic methods: A survey," *EAI Endorsed Trans. Energy Web*, vol. 7, no. 26, pp. 1–15, 2020.
[145] G. De La T. Parra, P. Rad, and K.-K. R. Choo, "Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 32–46, Jun. 2019.
[146] E. Batista, M. A. Moncusi, P. López-Aguilar, A. Martínez-Ballesté, and A. Solanas, "Sensors for context-aware smart healthcare: A security perspective," *Sensors*, vol. 21, no. 20, p. 6886, Oct. 2021.
[147] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and C. Maple, "Cyber resilience and incident response in smart cities: A systematic literature review," *Smart Cities*, vol. 3, no. 3, pp. 894–927, Aug. 2020.
[148] S. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt, "Bringing science to digital forensics with standardized forensic corpora," *Digit. Invest.*, vol. 6, pp. S2–S11, Sep. 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287609000346
[149] C. Grajeda, F. Breitinger, and I. Baggili, "Availability of datasets for digital forensics- and what is missing," *Digit. Invest.*, vol. 22, pp. S94–S105, Aug. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287617301913
[150] M. Köhn, M. S. Olivier, and J. H. Eloff, "Framework for a digital forensic investigation," in *Proc. ISSA*, 2006, pp. 1–7.
[151] W. Halboob and R. Mahmod, "State of the art in trusted computing forensics," in *Future Information Technology, Application, and Service*. Dordrecht, The Netherlands: Springer, 2012, pp. 249–258.
[152] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated digital forensic process model," *Comput. Secur.*, vol. 38, pp. 103–115, Oct. 2013.
[153] H. I. Bulbul, H. G. Yavuzcan, and M. Ozel, "Digital forensics: An analytical crime scene procedure model (ACSPM)," *Forensic Sci. Int.*, vol. 233, nos. 1–3, pp. 244–256, Dec. 2013.

[154] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–131, 2011.
[155] R. Adams, V. Hobbs, and G. Mann, "The advanced data acquisition model (Adam): A process model for digital forensic practice," *J. Digit. Forensics, Secur. Law*, vol. 8, no. 4, pp. 25–48, 2013.
[156] J. Williams, "ACPO good practice guide for digital evidence," Metrop. Police Service, Assoc. Chief Police Officers, GB, Tech. Rep., 2012.
[157] K. Kent, S. Chevalier, T. Grance, and H. Dang, "SP 800-86. guide to integrating forensic techniques into incident response," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2006.
[158] W. G. Kruse II and J. G. Heiser, *Computer Forensics: Incident Response Essentials*. London, U.K.: Pearson, 2001.
[159] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *Int. J. Digit. Evidence*, vol. 1, no. 3, pp. 1–12, 2002.
[160] B. Carrier and E. H. Spafford, "Getting physical with the investigative process," *Int. J. Digit. Evidence*, 2003.
[161] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," *Digit. Invest.*, 2004.
[162] S. O. Ciardhuáin, "An extended model of cybercrime investigations," *International Journal of Digital Evidence*, vol. 3, no. 1, pp. 1–22, 2004.
[163] I. O, D. Chris, and D. David, "A new approach of digital forensic model for digital forensic investigation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 12, pp. 175–178, 2011.
[164] (2020). European Network of Forensic Science Institutes. *Forensic Guidelines*. [Online]. Available: http://enfsi.eu/documents/forensic-guidelines/
[165] Y. Yusoff, R. Ismail, and Z. Hassan, "Common phases of computer forensics investigation models," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 17–31, 2011.
[166] K. Kyei, P. Zavarsky, D. Lindskog, and R. Ruhl, "A review and comparative study of digital forensic investigation models," in *Digital Forensics and Cyber Crime*, M. Rogers and K. C. Seigfried-Spellar, Eds. Berlin, Germany: Springer, 2013, pp. 314–327.
[167] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A blockchain-based chain of custody for evidences management in digital forensics," 2018, *arXiv:1807.10359*.
[168] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Inf. Sci.*, vol. 491, pp. 151–165, Jul. 2019.
[169] R. S. Greenfield *et al.*, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Boca Raton, FL, USA: CRC Press, 2002.
[170] D. Reilly, C. Wren, and T. Berry, "Cloud computing: Forensic challenges for law enforcement," in *Proc. Int. Conf. Internet Technol. Secured Trans.*, Nov. 2010, pp. 1–7.
[171] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, Aug. 2010.
[172] A. Guarino, "Digital forensics as a big data challenge," in *ISSE Securing Electronic Business Processes*. Wiesbaden, Germany: Springer, 2013, pp. 197–203.
[173] G. Mohay, "Technical challenges and directions for digital forensics," in *Proc. 1st Int. Workshop Systematic Approaches to Digit. Forensic Eng. (SADFE)*, Nov. 2005, pp. 155–161.
[174] Z. Li, Q. A. Chen, R. Yang, Y. Chen, and W. Ruan, "Threat detection and investigation with system-level provenance graphs: A survey," *Comput. Secur.*, vol. 106, Jul. 2021, Art. no. 102282.
[175] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A review of mobile forensic investigation process models," *IEEE Access*, vol. 8, pp. 173359–173375, 2020.
[176] M. Abulaish and N. A. H. Haldar, "Advances in digital forensics frameworks and tools: A comparative insight and ranking," *Int. J. Digit. Crime Forensics*, vol. 10, no. 2, pp. 95–119, 2018.
[177] R. Agarwal and S. Kothari, "Review of digital forensic investigation frameworks," in *Information Science and Applications* (Lecture Notes in Electrical Engineering), vol. 339. Berlin, Germany: Springer-Verlag, 2015, pp. 561–571.
[178] P. Amann and J. I. James, "Designing robustness and resilience in digital investigation laboratories," *Digit. Invest.*, vol. 12, pp. S111–S120, Mar. 2015.
[179] R. Montasari, "An ad hoc detailed review of digital forensic investigation process models," *Int. J. Electron. Secur. Digit. Forensics*, vol. 8, no. 3, pp. 205–223, 2016.
[180] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. J. Cano, "Digital forensic analysis of cybercrimes: Best practices and methodologies," *Int. J. Inf. Secur. Privacy*, vol. 11, no. 2, pp. 25–37, 2017.
[181] *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, Joint Technical Committee ISO/IEC JTC, International Organization for Standardization, Geneva, CH, Standard ISO/IEC 27037:2012, 2012. [Online]. Available: https://www.iso.org/standard/44381.html
[182] European Telecommunications Standards Institute. (2020). *Techniques for Assurance of Digital Material Used in Legal Proceedings—ETSI TS 103 643 v1.1.1 (2020-01)*. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103600_103699/103643/01.01.01_60/t%s_103643v010101p.pdf
[183] K. Kent, S. Chevalier, T. Grance, and H. Dang, "SP 800-86. guide to integrating forensic techniques into incident response," Nat. Inst. Standards Technol., Tech. Rep., 2006.
[184] R. Ayers, S. Brothers, and W. Jansen. (May 2014). *Guidelines on Mobile Device Forensics*. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final
[185] L. Wilson-Wilde, "The international development of forensic science standards—A review," *Forensic Sci. Int.*, vol. 288, pp. 1–9, Jul. 2018.
[186] M. Robinson. (2015). *Digital Forensics Workbook: Hands-on Activities in Digital Forensics*. CreateSpace Independent Publishing Platform. [Online]. Available: https://books.google.gr/books?id=4dyHjgEACAAJ
[187] J. Tan, *Forensic Readiness*. Cambridge, MA, USA: Stake, 2001, pp. 1–23.
[188] K. Reddy and H. S. Venter, "The architecture of a digital forensic readiness management system," *Comput. Secur.*, vol. 32, pp. 73–89, Feb. 2013.
[189] M. Elyas, A. Ahmad, S. B. Maynard, and A. Lonie, "Digital forensic readiness: Expert perspectives on a theoretical framework," *Comput. Secur.*, vol. 52, pp. 70–89, Jul. 2015.
[190] B. Endicott-Popovsky, N. Kuntze, and C. Rudolph, "Forensic readiness: Emerging discipline for creating reliable and secure digital evidence," *J. Harbin Inst. Technol.*, vol. 22, no. 1, pp. 1–8, 2015.
[191] A. Mouhtaropoulos, C. T. Li, and M. Grobler, "Digital forensic readiness: Are we there yet?" *J. Int. Commercial Law Technol.*, vol. 9, no. 3, pp. 173–179, 2014.
[192] A. M. Marshall and R. Paige, "Requirements in digital forensics method definition: Observations from a U.K. study," *Digit. Invest.*, vol. 27, pp. 23–29, Dec. 2018.
[193] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington, "A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later," *Comput. Secur.*, vol. 57, pp. 1–13, Mar. 2016.
[194] M. Ozel, H. I. Bulbul, H. G. Yavuzcan, and O. F. Bay, "An analytical analysis of Turkish digital forensics," *Digit. Invest.*, vol. 25, pp. 55–69, Jun. 2018.
[195] S. Park, N. Akatyev, Y. Jang, J. Hwang, D. Kim, W. Yu, H. Shin, C. Han, and J. Kim, "A comparative study on data protection legislations and government standards to implement digital forensic readiness as mandatory requirement," *Digit. Invest.*, vol. 24, pp. S93–S100, Mar. 2018.
[196] H. Arshad, A. B. Jantan, and O. I. Abiodun, "Digital forensics: Review of issues in scientific validation of digital evidence," *J. Inf. Process. Syst.*, vol. 14, no. 2, pp. 346–376, 2018.
[197] A. Butler and K.-K.-R. Choo, "IT standards and guides do not adequately prepare IT practitioners to appear as expert witnesses: An Australian perspective," *Secur. J.*, vol. 29, no. 2, pp. 306–325, Apr. 2016.
[198] A. S. Bali, G. Edmond, K. N. Ballantyne, R. I. Kemp, and K. A. Martire, "Communicating forensic science opinion: An examination of expert reporting practices," *Sci. Justice*, vol. 60, no. 3, pp. 216–224, May 2020.
[199] L. M. Howes and N. Kemp, "Discord in the communication of forensic science: Can the science of language help foster shared understanding?" *J. Lang. Social Psychol.*, vol. 36, no. 1, pp. 96–111, Jan. 2017.
[200] L. M. Howes, K. P. Kirkbride, S. F. Kelty, R. Julian, and N. Kemp, "The readability of expert reports for non-scientist report-users: Reports of forensic comparison of glass," *Forensic Sci. Int.*, vol. 236, pp. 54–66, Mar. 2014.
[201] L. M. Howes, K. P. Kirkbride, S. F. Kelty, R. Julian, and N. Kemp, "Forensic scientists' conclusions: How readable are they for non-scientist report-users?" *Forensic Sci. Int.*, vol. 231, nos. 1–3, pp. 102–112, Sep. 2013.

[202] M. A. K. Halliday, "Some grammatical problems in scientific English," *Genre Systemic Funct. Stud.*, vol. 6, pp. 13–37, Jan. 1989.
[203] S. Eggins, *Introduction to Systemic Functional Linguistics*. A&C Black, 2004.
[204] R. Flesch, "A new readability yardstick," *J. Appl. Psychol.*, vol. 32, no. 3, p. 221, 1948.
[205] R. Flesch and A. J. Gould, *The Art Readable Writing*, vol. 8. New York, NY, USA: Harper, 1949.
[206] J. P. Kincaid, R. P. Fishburne, Jr., R. L. Rogers, and B. S. Chissom, "Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel," Naval Tech. Training Command Millington TN Res. Branch, Tech. Rep., 1975.
[207] R. Clerehan, R. Buchbinder, and J. Moodie, "A linguistic framework for assessing the quality of written patient information: Its use in assessing methotrexate information for rheumatoid arthritis," *Health Educ. Res.*, vol. 20, no. 3, pp. 334–344, Jun. 2005.
[208] P. B. Mosenthal and I. S. Kirsch, "A new measure for assessing document complexity: The pmose/ikirsch document readability formula," *J. Adolescent Adult Literacy*, vol. 41, no. 8, pp. 638–657, 1998.
[209] J. L. Calderón, E. Fleming, M. R. Gannon, S.-C. Chen, J. A. Vassalotti, and K. C. Norris, "Applying an expanded set of cognitive design principles to formatting the kidney early evaluation program (KEEP) longitudinal survey," *Amer. J. Kidney Diseases*, vol. 51, no. 4, pp. S83–S92, Apr. 2008.
[210] M. Graves and B. Graves, "Assessing text difficulty and accessibility," in *Scaffolding Reading Experiences: Designs for Student Success*. Norwood, MA, USA: Christopher-Gordon, 2003.
[211] J. Cosic, "Formal acceptability of digital evidence," in *Multimedia Forensics and Security*. Cham, Switzerland: Springer, 2017, pp. 327–348.
[212] O. Sallavaci and C. George, "Procedural aspects of the new regime for the admissibility of expert evidence: What the digital forensic expert needs to know," *Int. J. Electron. Secur. Digit. Forensics*, vol. 5, nos. 3–4, pp. 161–171, 2013.
[213] P. Sommer, "Certification, registration and assessment of digital forensic experts: The U.K. experience," *Digit. Invest.*, vol. 8, no. 2, pp. 98–105, Nov. 2011.
[214] D. Garrie. (2016). *The Neutral Corner: Understanding a Digital Forensics Report*. [Online]. Available: https://www.legalexecutiveinstitute.com/understanding-digital-forensics% -report/
[215] H. Bariki, M. Hashmi, and I. Baggili, "Defining a standard for reporting digital evidence items in computer forensic tools," in *Proc. Int. Conf. Digit. Forensics Cyber Crime*. Berlin, Germany: Springer, 2010, pp. 78–95.
[216] N. M. Karie, V. R. Kebande, H. S. Venter, and K.-K.-R. Choo, "On the importance of standardising the process of generating digital forensic reports," *Forensic Sci. Int., Rep.*, vol. 1, Nov. 2019, Art. no. 100008.
[217] D. Klitou, "Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century," *Legisprudence*, vol. 5, no. 3, pp. 297–329, 2011.
[218] N. Daniels, "Justice, health, and healthcare," *Amer. J. Bioethics*, vol. 1, no. 2, pp. 2–16, Feb. 2001.
[219] M. Neocleous, "Security, liberty and the myth of balance: Towards a critique of security politics," *Contemp. Political Theory*, vol. 6, no. 2, pp. 131–149, May 2007.
[220] (2004). Council of Europe. *Details of treaty no. 185*. [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/1% 85
[221] (1962). C. of Europe. *Details of Treaty no. 030*. [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/0% 30
[222] (2013). C. of Europe. *Data Protection and Cybercrime Division, Electronic Evidence Guide*. [Online]. Available: https://rm.coe.int/16803028af
[223] (2018). C. of Europe. *Towards a Protocol to the Budapest Convention*. [Online]. Available: https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713
[224] (2016). E. Union. *Directive (EU) 2016/680 of the European Parliament and of the Council*. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680
[225] E. Union. (2014). *Regulation (EU) no 910/2014, of the European Parliament and of the Council*. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.201% 4.257.01.0073.01.ENG
[226] (2019). European Commission. *E-evidence—Cross-Border Access to Electronic Evidence*. [Online]. Available: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/crimi%nal-justice/e-evidence-cross-border-access-electronic-evidence_en
[227] (2016). European Union. *Regulation (EU) 2016/95 of the European Parliament and of the Council*. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0095
[228] (2017). E. Union. *Final Report Summary—European Informatics Data Exchange Framework for Courts and Evidence*. [Online]. Available: https://cordis.europa.eu/project/id/608185/reporting
[229] F. Insa, "The admissibility of electronic evidence in court (A.E.E.C.): Fighting against high-tech crime—Results of a European study," *J. Digit. Forensic Pract.*, vol. 1, no. 4, pp. 285–289, Jun. 2007.
[230] M. A. Biasiotti, J. P. M. Bonnici, J. Cannataci, and F. Turchi, *Handling and Exchanging Electronic Evidence Across Europe*. vol. 39. Cham, Switzerland: Springer, 2018.
[231] *Electronic Evidence—A basic Guide for First Responders*, Eur. Netw. Inf. Secur. Agency (ENISA), Athens, Greece, 2015.
[232] R. Marty, "Cloud application logging for forensics," in *Proc. ACM Symp. Appl. Comput. (SAC)*, 2011, pp. 178–184.
[233] P. Trenwith and H. Venter, "Digital forensic readiness in the cloud," in *Proc. IEEE Information Security for South Africa*, 2013, pp. 1–5.
[234] A. Patrascu and V.-V. Patriciu, "Logging system for cloud computing forensic environments," *J. Control Eng. Appl. Informat.*, vol. 16, no. 1, pp. 80–88, 2014.
[235] V. Kebande and H. Venter, "A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis," in *Proc. Eur. Conf. Cyber Warfare Secur.*, 2015, p. 373.
[236] S. Zawoad, A. K. Dutta, and R. Hasan, "Towards building forensics enabled cloud through secure logging-as-a-service," *IEEE Trans. Depend. Sec. Comput.*, vol. 13, no. 2, pp. 148–162, Mar./Apr. 2016.
[237] M. A. M. Ahsan, A. W. B. A. Wahab, M. Y. I. B. Idris, S. Khan, E. Bachura, and K.-K.-R. Choo, "CLASS: Cloud log assuring soundness and secrecy scheme for cloud forensics," *IEEE Trans. Sustain. Comput.*, vol. 6, no. 2, pp. 184–196, Apr. 2021.
[238] H. Tian, J. Wang, C.-C. Chang, and H. Quan, "Public auditing of log integrity for shared cloud storage systems via blockchain," *Wireless Netw.*, vol. 2020, pp. 378–387, May 2020.
[239] F. Casino, E. Politou, E. Alepis, and C. Patsakis, "Immutability and decentralized storage: An analysis of emerging threats," *IEEE Access*, vol. 8, pp. 4737–4744, 2020.
[240] V. R. Kebande, R. A. Ikuesan, and N. M. Karie, "Review of blockchain forensics challenges," in *Blockchain Security in Cloud Computing*. Cham, Switzerland: Springer, 2022, pp. 33–50.
[241] S. T. Ali, P. McCorry, P. H.-J. Lee, and F. Hao, "ZombieCoin 2.0: Managing next-generation botnets using bitcoin," *Int. J. Inf. Secur.*, vol. 17, no. 4, pp. 411–422, Aug. 2018.
[242] C. Patsakis and F. Casino, "Hydras and IPFS: A decentralised playground for malware," *Int. J. Inf. Secur.*, vol. 18, no. 6, pp. 787–799, Dec. 2019.
[243] (2020). O. Caspi. *Trickbot Bazarloader in-Depth* [Online]. Available: https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-% in-depth
[244] F. Casino, N. Lykousas, V. Katos, and C. Patsakis, "Unearthing malicious campaigns and actors from the blockchain DNS ecosystem," *Comput. Commun.*, vol. 179, pp. 217–230, Nov. 2021.
[245] T. de Balthasar and J. Hernandez-Castro, "An analysis of bitcoin laundry services," in *Secure IT Systems* (Lecture Notes in Computer Science), H. Lipmaa, A. Mitrokotsa, and R. Matulevicius, Eds., vol. 10674. Springer, 2017, pp. 297–312, doi: 10.1007/978-3-319-70290-2_18.
[246] G. Kumar, R. Saha, C. Lal, and M. Conti, "Internet-of-forensic (IoF): A blockchain based digital forensics framework for iot applications," *Future Gener. Comput. Syst.*, vol. 120, pp. 13–25, 2021.
[247] (2019). *LOCARD: Lawful Evidence Collecting and Continuity Platform Development*. [Online]. Available: https://locard.eu
[248] L. Zarpala and F. Casino, "A blockchain-based forensic model for financial crime investigation: The embezzlement scenario," *Digit. Finance*, vol. 3, no. 3, pp. 1–32, 2021.
[249] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020.
[250] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.

[251] L. Ogiela and M. R. Ogiela, "Cognitive security paradigm for cloud computing applications," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 8, p. e5316, Apr. 2020.
[252] K. Demertzis, P. Kikiras, N. Tziritas, S. Sanchez, and L. Iliadis, "The next generation cognitive security operations center: Network flow forensics using cybersecurity intelligence," *Big Data Cognit. Comput.*, vol. 2, no. 4, p. 35, Nov. 2018.
[253] S. Schuster, M. van den Berg, X. Larrucea, T. Slewe, and P. Ide-Kostic, "Mass surveillance and technological policy options: Improving security of private communications," *Comput. Standards Interfaces*, vol. 50, pp. 76–82, Feb. 2017.
[254] D. J. Bernstein, T. Lange, and R. Niederhagen, "Dual EC: A standardized back door," in *The New Codebreakers*. Berlin, Germany: Springer, 2016, pp. 256–281.
[255] M. Smith and M. Green, "A discussion of surveillance backdoors: Effectiveness, collateral damage and ethics," in *Proc. Int. Secur. 21st Century, Germany's Int. Responsibility*, 2016, pp. 131–142.
[256] E. Rice, "The second amendment and the struggle over cryptography," *Hastings Sci. Tech. LJ*, vol. 9, p. 29, Oct. 2017.
[257] A. M. Dunn, O. S. Hofmann, B. Waters, and E. Witchel, "Cloaking malware with the trusted platform module," in *Proc. 20th USENIX Secur. Symp. (USENIX Security)*, San Francisco, CA, USA, Aug. 2011, pp. 1–16. [Online]. Available: https://www.usenix.org/conference/usenix-security-11/cloaking-malware-t% rusted-platform-module
[258] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," *IEEE access*, vol. 6, pp. 52138–52160, 2018.
[259] (2020). The European Union Agency for Cybersecurity (ENISA). *Guideline on Security Measures Under the EECC*. [Online]. Available: https://www.enisa.europa.eu/publications/guideline-on-security-measures% -under-the-eecc/
[260] (2020). The European Union Agency for Cybersecurity (ENISA). *5G supplement—To the Guideline on Security Measures Under the EECC*. [Online]. Available: https://www.enisa.europa.eu/publications/5g-supplement-security-measure% s-under-eecc/
[261] (2020). N. I. of Standards and Technology. *SP 800-124 rev. 2—Guidelines for Managing the Security of Mobile Devices in the Enterprise*. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft
[262] (2020). National Institute of Standards and Technology. *NIST Releases Draft Guidance on Internet of Things Device Cybersecurity*. [Online]. Available: https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guida% nce-internet-things-device-cybersecurity
[263] The European Union Agency for Cybersecurity (ENISA). *Guidelines for securing the Internet of Things*. (2020). [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-in% ternet-of-things
[264] (2017). The European Union Agency for Cybersecurity (ENISA). *Guidelines for SMES on the Security of Personal Data Processing*. [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-sec% urity-of-personal-data-processing
[265] (2020). *National Institute of Standards and Technology. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*. [Online]. Available: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%% 20Framework_V1.0.pdf
[266] (2019). National Institute of Standards and Technology. *Recommendations on Shaping technology According to GDPR Provisions—Exploring the Notion of Data Protection by Default*. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-on-shaping-tec% hnology-according-to-gdpr-provisions-part-2
[267] A. Zigomitros, F. Casino, A. Solanas, and C. Patsakis, "A survey on privacy properties for data publishing of relational data," *IEEE Access*, vol. 8, pp. 51071–51099, 2020.
[268] (2019). The European Union Agency for Cybersecurity (ENISA). *Towards a Framework for Policy Development in Cybersecurity—Security and Privacy Considerations in Autonomous Agents*. [Online]. Available: https://www.enisa.europa.eu/publications/considerations-in-autonomous-a% gents
[269] H. Arshad, E. Omlara, I. O. Abiodun, and A. Aminu, "A semi-automated forensic investigation model for online social networks," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101946.
[270] N. Sunde and G. Horsman, "Part 2: The phase-oriented advice and review structure (PARS) for digital forensic investigations," *Forensic Sci. International: Digit. Invest.*, vol. 36, Mar. 2021, Art. no. 301074.

FRAN CASINO (Member, IEEE) received the B.Sc. degree in computer science, the M.Sc. degree in computer security and intelligent systems, and the Ph.D. degree *(cum laude)* in computer science from Rovira i Virgili University, Tarragona, Catalonia, Spain, in 2010, 2013, and 2017, respectively. He was a Visiting Researcher at ISCTE-IUL, Lisbon, in 2016. He has participated in several European-, Spanish-, and Catalan-funded research projects, and he has authored more than 50 publications in peer-reviewed international conferences and journals. He is a Postdoctoral Researcher with the Department of Computer Engineering and Mathematics, Rovira i Virgili University, and the Athena Research Center, Athens, Greece. His research interests include pattern recognition, and data management applied to different fields such as privacy and security protection, recommender systems, smart health, supply chain, and blockchain. He received the Best Dissertation Award from Rovira i Virgili University.

THOMAS K. DASAKLIS received the bachelor's degree from the Department of Industrial Management and Technology, University of Piraeus, and the M.Sc. degree in supply chain management and the Ph.D. degree in emergency supply chain management and disaster response from the University of Piraeus. He has worked for the European Commission (DG Humanitarian Aid and Civil Protection) and the University of Piraeus Research Centre. He has also worked in the private sector for three years as the Supply Chain Director. He has participated in National and European research projects and has published papers in books, peer reviewed journals, and conference proceedings. He is currently an Assistant Professor with the School of Social Sciences, Hellenic Open University. His research interests include in the area of supply chain management, operational research, humanitarian logistics/disaster response, data analysis, and blockchain technology. He has served as a guest editor, a Program Committee Member, and a reviewer for various international journals and conferences.

GEORGIOS P. SPATHOULAS received the Diploma of Electrical and Computer Engineering degree from the Aristotle University of Thessaloniki, in 2002, the M.Sc. degree in computer science from The University of Edinburgh, in 2005, and the Ph.D. degree from the Department of Digital Systems, University of Piraeus, in 2013. He is a member of Laboratory Teaching Staff of the Department of Computer Science and Biomedical Informatics, University of Thessaly, since 2014, and he teaches in both undergraduate and postgraduate study programs of the department. He is also a Postdoctoral Researcher with the Critical Infrastructures Security and Resilience Group at the Center for Cyber and Information Security (CCIS), Norwegian University of Science and Technology (NTNU). He is the coauthor of more than 30 publications in peer reviewed journals and conference proceedings. His research interests include related to networks security, privacy preserving techniques, and blockchain technology. He has also served as the Program Committee Member for international conferences and has taken part in both national and international research programs.

MARIOS ANAGNOSTOPOULOS received the master's degree in information and communication systems security and the Ph.D. degree in information and communication systems engineering from the University of the Aegean, Greece. He has worked as a Postdoctoral Research Fellow in cyber security at the Norwegian University of Science and Technology (NTNU) and the Singapore University of Technology and Design (SUTD). He has joined the Department of Electronic Systems, Aalborg University, Copenhagen, as an Assistant Professor at the Communication, Media and Information Technologies Section, Aalborg University, and is a member of the Cyber-Security Research Group. He is the coauthor of more than 20 publications in peer-reviewed international conferences and journals. His research interests include the area of networks and computer security, and specifically DNS security, denial of service attacks, malware analysis, and forensics. He has also served as a Program Committee Member for international conferences and has taken part in both national and international research programs.

AMRITA GHOSAL received the Ph.D. degree in computer science and engineering from the Indian Institute of Engineering Science and Technology, India, in 2015. After her Ph.D. degree, she worked as a Postdoctoral Researcher at the Department of Mathematics, University of Padua, Italy. She is currently a Marie Skłodowska-Curie Fellow with the Department of Electronic and Computer Engineering, University of Limerick, Ireland. She has coauthored a number of book chapters. Her research interests include in the areas of security and privacy for mobile and wireless networks. Particularly, she is interested in detection, prevention, and mitigation of different DoS style attacks for smart grid, v2x, connected vehicle, cyber-physical systems, and the IoT. In these areas, she has published more than 35 papers in high quality journals and refereed conference proceedings.

ISTVÁN BOŘOCZ received the Law (JD) and postgraduate specialist Diploma degrees in information and communication technology law from the University of Pécs, in 2013 and 2015, respectively, and the LLM degree in law and technology from Tilburg University, in 2016. He is a Data Protection Officer at Ion Beam Applications SA (IBA) and a Researcher at the Research Group on Law, Science, Technology and Society (LSTS). He is also a member of the Health and Ageing Law Laboratory (HALL), a spinoff group within LSTS. He is involved and provides legal assistance in several EU co-funded research projects, such as ARC, LOCARD, PERSONA, STAR, INTREPID, MaTHiSiS, FORENSOR, HR-Recycler, and SUCCESS or PARENT. These projects target a range of areas, such as law enforcement, technology-induced education, human–robot interaction, smart cities, or helping the work of data protection authorities. He is a member of the Ethical Advisory Board of the Horizon2020 Project CUIDAR. His research interests include the notion of the privacy of the mind along with the legal, theoretical, and practical issues of human enhancement technologies, with special focus on cognitive enhancement. In particular, he focuses on technologies which passively read and actively affect the human brain and the mind both within and outside the field of health care. He is also an Editor of the World Law Dictionary, developed by TransLegal Sweden AB.

AGUSTI SOLANAS (Senior Member, IEEE) received the M.Sc. degree (Hons.) in computer engineering from Rovira i Virgili University (URV), in 2004, the Diploma degree in advanced studies from the Polytechnic University of Catalonia, in 2005, and the Ph.D. degree from the Department of Telematics Engineering, Polytechnic University of Catalonia, in 2007. He is currently a Professor with the Department of Computer Engineering and Mathematics and the Head of the Smart Technologies Research Group, URV. He serves as a Scientific Coordinator for APWG.EU. His current research interests include smart technologies, health informatics, behavior analysis, multivariate analysis, privacy protection, and computer security.

MAURO CONTI (Fellow, IEEE) received the Ph.D. degree from the Sapienza University of Rome, Italy, in 2009. After his Ph.D. degree, he was a Postdoctoral Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined as an Assistant Professor at the University of Padua, Italy, where he became an Associate Professor, in 2015, and a Full Professor, in 2018. He has been a Visiting Researcher with GMU, UCLA, UCI, TU Darmstadt, UF, and FIU. He is a Full Professor with the University of Padua. He is also affiliated with the Delft University of Technology (TU Delft) and the University of Washington, Seattle. His research is funded by companies, including Cisco, Intel, and Huawei. His main research interests include security and privacy. In these areas, he has published more than 400 papers in topmost international peer-reviewed journals and conferences. He is a Senior Member of the ACM and a fellow of the Young Academy of Europe. He has been awarded with a Marie Curie Fellowship by the European Commission, in 2012, and with a Fellowship by the German DAAD, in 2013. He was the Program Chair of TRUST 2015, ICISS 2016, WiSec 2017, ACNS 2020, and CANS 2021, and the General Chair for SecureComm 2012, SACMAT 2013, NSS 2021, and ACNS 2022. He is the Editor-in-Chief of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the Area Editor-in-Chief of IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, and he has been an Associate Editor of several journals, including IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT.

CONSTANTINOS PATSAKIS received the B.Sc. degree in mathematics from the University of Athens, Greece, the M.Sc. degree in information security from the Royal Holloway, University of London, and the Ph.D. degree in cryptography and malware from the Department of Informatics, University of Piraeus. He has participated in several national (Greek, Spanish, Catalan, and Irish) and European research and development projects (e.g., TACTICS, MITIGATE, OPERANDO, SAURON, PRACTICIES, and YAKSHA). He worked as a Researcher at the UNESCO Chair in data privacy and as a Research Fellow at the Trinity College Dublin, Dublin, Ireland. His main research interests include cryptography, malware, security, privacy, and data anonymization. Currently, he is Assistant Professor at University of Piraeus and adjunct researcher of Athena Research and Innovation Center.