A socio-technical perspective on forensic challenges in smartphones and smartwatches: A systematic literature review*

Jonas Ingemarsson[1,*,†], Erik Andersson[1,†], Joakim Kävrestad[2] and Marcus Birath[1]

[1]University of Skövde, Högskolevägen 1, 541 28 Skövde, Sweden
[2]Jönköping School of Engineering, Jönköping University, Gjuterigatan 5, 553 18 Jönköping, Sweden

Abstract

With the increasing use of smartphones and smartwatches, these devices have become vital sources of digital evidence in forensic investigations, as they often act as "*silent witnesses*" to events. Thus, it is important to understand the unique challenges they pose—individually and in combination.

This paper reports on a systematic literature review to examine how these devices relate to current forensic challenges, identify potential differences between the devices and future research needs. From 73 relevant articles, thematic analysis identified four main themes and related sub-themes for each device. The review considers not only technical constraints, but also the broader context in which these devices are used and investigated, offering a socio-technical lens on digital forensics.

The findings shows that challenges related to smartphones are more frequently discussed than those to smartwatches. This may be due either to smartphones' greater complexity or to limited research on smartwatches—the latter being more likely based on the volume of published work.

This review provides a structured overview of the forensic landscape and identifies key gaps for future study.

Keywords

Digital forensics, smartphones, smartwatches, forensic challenges

1. Introduction

In digital forensics, smartphones and smartwatches have become valuable sources of evidence in crime and incident investigations. In addition to be carriers of traditional forensic artifacts such as communication data and pictures, they are often so called "*slient witnesses*" of crimes. For instance, in the Caroline Crouch case, data from her smartwatch showed heartbeats after her husband claimed she was dead, while his phone showed movement despite claiming to be tied up [1, 2]. This type of data, called gait or sensor data, is collected by the devices without actions needed on the part of the user. Such data can, as in the Caroline Crouch case, provide key evidence in criminal investigation. How gait data is stored can differ between devices and application. It is, for instance, common that a smartwatch maintains some limited internal memory while continuously synchronizing with a smartphone or cloud service. Consequently, we consider both smartwathches and smartphones in this research.

Reliable figures on smartwatch adoption remain unclear. Laricchia [3] forecasted 225 million users in 2024, while others estimate nearly double that [4, 5]. Smartwatches collect health-related and notification data [6], and with over 5.31–5.75 billion smartphone users worldwide [7, 8], both device types are crucial in forensic investigations as these devices can store key digital evidence [9, 10, 7].

Given their widespread use, it is important to understand the challenges of investigating these devices, but also the difference between them. This study investigates these differences by conducting a systematic literature review, identifying current challenges, gaps, and future research opportunities.

11th International Workshop on Socio-Technical Perspectives in IS (STPIS'25), Ss. Cyril and Methodius University, North Macedonia

*Corresponding author.
†These authors contributed equally.
$jonas.ingemarsson@his.se (J. Ingemarsson); joakim.kavrestad@ju.se (J. Kävrestad); marcus.birath@his.se (M. Birath)
https://www.his.se (J. Ingemarsson); https://ju.se (J. Kävrestad); https://www.his.se (M. Birath)
0009-0004-0326-2548 (J. Ingemarsson); 0000-0003-2084-9119 (J. Kävrestad); 0000-0001-5692-4008 (M. Birath)

While smartphones are well-studied, smartwatch forensics is emerging. A systematic literature review is appropriate for synthesizing available research.

This study follows the three-phase model by Kitchenham and Charters [11], incorporating the six steps by Paré and Kitsiou [12], and uses thematic analysis [13] to identify challenge patterns. The analysis adopts a socio-technical lens where we perceive digital forensics as a socio-technical process. While the technical capability to extract and analyze digital information is central, forensic capabilities are impacted by social aspects including regulations as well as formal and informal organizational structures.

The remainder of this paper is structured as follows: Section 2 provides background on the topic, introducing key concepts and establishing a solid foundation for understanding the results and conclusions. Section 3 outlines the methodology used in this study, which is a structured literature review. It details the process of data collection and analysis. Section 4 presents the findings, including the results of the thematic coding and the main research insights. In Section 5, the results are discussed, including the researchers' reflections and elaborating on the socio-technical dimensions of the study—highlighting a paradox. Section 6 answers the research question by presenting the conclusions and limitations of the study. Finally, Section 7 outlines directions for future research.

2. Background

2.1. Smartphones

Due to their widespread use and multifunctionality, smartphones are valuable sources of digital evidence in forensic investigations. Despite differences in brand, OS, and hardware, they typically contain similar categories of data: internal storage, SIM information, messages, location, social media activity, call logs, multimedia, and network data [14].

Smartphones also collect gait data—patterns of human movement such as walking or climbing stairs. This data, captured through sensors like accelerometers and gyroscopes, is known as on-body gait and is stored by *Inertial Measurement Units* (IMUs) embedded in smartphones and smartwatches [15]. These always-on sensors can without drawing attention capture continuous motion data [16]. Because gait cycles are unique to individuals, this data can be used for biometric identification [17, 18]. Gait-based biometrics are already applied in forensic contexts for identification and verification. For instance, Ghosh et al. [19] found that gait patterns while walking and typing, as recorded by smartphones, could help identify individuals and infer demographic traits like age and gender.

2.2. Smartwatches

Smartwatches are wearable devices that extend smartphone functionalities and offer real-time access to data, apps, and notifications [20, 21]. Unlike traditional watches, they can run mobile applications, provide fitness tracking, and support messaging and calls. Their popularity has grown significantly over the past decade [20].

Smartwatches collect substantial personal data through sensors, including heart rate, steps, and location. This data can be useful in forensic investigations [22, 6]. Stored information may include messages, contacts, call logs, notifications, and health metrics [6, 23, 24]. Location data from GPS and movement records can also help verify or disprove alibis [25, 26].

Like smartphones, smartwatches contain sensors such as accelerometers and gyroscopes, which can capture gait data for biometric identification [27, 28, 29]. Their consistent position on the body improves gait measurement accuracy. Other sensors-like heart rate monitors, GPS, microphones, and ambient light sensors—add further forensic value [30]. For example, smartwatch data was used in a rape case where the movement recorded contradicted the reported timeline, resulting in charges against the complainant [26, 31].

Because smartwatches operate passively in the background, they continuously collect potentially incriminating or exonerating evidence, such as physical activity or physiological data. These digital

traces are increasingly relevant in cases involving suspicious deaths, aviation incidents, and legal disputes [30, 32].

2.3. Gait data

Both smartphones and smartwatches are equipped with sensors such as accelerometers, which collect gait—or sensory—data. This data can support or refute alibis and contribute to hypothesis development in digital investigations [33]. These sensors provide both direct evidence, like GPS location, and indirect evidence, such as determining whether someone is indoors based on light sensor data.

Modern personal devices store large volumes of sensory information, particularly IMU data, which can be used for biometric identification through gait analysis. Gait refers to movement patterns such as walking or climbing stairs and can be classified into two types: visual gait, captured via external cameras, and on-body gait, collected by sensors embedded in devices worn on the body [15].

As users carry or wear these devices daily, they continuously log data useful for activity recognition, health monitoring, and authentication [15]. Gait analysis has proven valuable in criminal investigations, as demonstrated in a case where gait patterns helped identify and convict a bank robber [34].

2.4. Digital evidence

Digital evidence is relevant in nearly all types of crimes—whether cyber-related or traditional—since modern life constantly generates digital traces [35, 36, 37]. Even crimes committed offline may leave behind digital records, such as CCTV footage, GPS logs, transit receipts, or photos taken by bystanders [36].

Devices like smartphones often contain digital evidence, including location data, messages, call logs, and photos. They also gather sensory data such as activity recognition and gait patterns [35]. Similarly, smartwatches can hold information like heart rate, step count, messages, emails, and other personal data [38].

Harbawi and Varol [25] defines digital evidence as any data transferred through an electronic system. This may include documents, videos, browsing histories, social media activity, financial records, e-signatures, or even online appointments.

2.5. Digital forensics

Digital forensics involves identifying "*what has happened*" by analyzing digital devices for evidence of criminal activity [36]. Flaglien et al. [39] describes it as a science-based process to preserve, collect, examine, and present digital evidence to reconstruct events or predict unauthorized actions.

As society becomes more digitized, digital forensics plays a role in most legal cases, involving data from smartphones, emails, GPS logs, or credit card transactions. Due to the volatility of some evidence types, standardized tools and procedures are essential [39].

In smartphone forensics, standard techniques apply, but should also include data specific to mobile devices, such as gait and sensor data [35]. For smartwatches, however, no universal forensic standard exists [40, 36]. Researchers propose custom frameworks for these devices [22, 6, 40], often placing them within IoT forensics [24, 41], which is defined as: "*an especial branch of digital forensics, where the identification, collection, organization, and presentation processes deal with the IoT infrastructures to establish the facts about a criminal incident*" [42, p.280].

2.5.1. The digital forensics process

Digital forensics involves collecting, analyzing, and reporting on digital data [36]. The process is generally divided into three phases, each described below.

Collect (Phase 1): This phase involves obtaining digital evidence from a target person, device, or location. Typically executed under a search warrant, investigators search for digital devices like smartphones, smartwatches, or hard drives that may hold relevant data [36].

Analyze (Phase 2): Here, forensic experts examine the collected data to reconstruct events or understand digital activity. This analysis is guided by specific questions from investigators, which help define the scope and legal boundaries of the examination [36].

Report (Phase 3): The final phase presents the findings in response to the investigator's questions. It is important to clearly distinguish facts from conclusions. This phase may prompt new questions, making the analysis and reporting stages iterative [36].

3. Methodology

Based on the purpose of this study, a structured literature review was conducted following the three phases proposed by Kitchenham and Charters [11] and the six-step approach outlined by Paré and Kitsiou [12]. To identify relevant literature, two search queries were constructed. The queries used were *(smartwatches OR "smart watches")* and *(smartphones OR "smart phones")*, both followed by *AND ("digital forensics" OR forensics OR forensic).* The intention was to capture as much relevant literature as possible, regardless of the specific combination used. References to challenges, obstacles, and similar concepts were intentionally omitted from the search strings in order to also retrieve articles where such challenges were identified as byproducts of research in the field.

The search strings were applied in five databases on 23 March 2025: ACM Digital Library, Emerald insight, IEEE Xplore, Scopus, and Web of Science. The search was restricted to include only conference papers and journal articles published from 2020 onward. Papers failing to meet the following inclusion criteria were excluded: peer-reviewed, written in English, and relevant to the topic, i.e., identifying current challenges. Articles with a primary focus other than smartwatches and/or smartphones were removed (e.g., those focusing on forensic identification or authentication of specific media types such as PRNU-based image source identification). Previous review articles were included in this study—but only if data could be extracted from their primary data.

Further, the screening process was carefully documented using a PRISMA flowchart (Figure 1), based on procedures established by Page et al. [43] and generated using a tool developed by Haddaway et al. [44]. The papers included in the study were analysed using thematic coding [13], as follows[1]:

1. Each paper was read in its entirety, and relevant sections were marked with labels (codes) that emerged inductively from the data.
2. Codes that related to one another were grouped into broader sub-themes, which also emerged inductively from the data.
3. Sub-themes that shared conceptual similarities were then merged into overarching themes, which likewise emerged inductively from the data.

The articles cited in the results are those that passed this review and coding process.

4. Results

This section presents the four identified themes from the thematic analysis for both smartphones and smartwatches, along with their associated sub-themes and codes. In total, eight sub-themes were identified for smartphones and seven for smartwatches. For both technologies, the theme *legal challenges* includes only a single code and therefore no sub-theme was formed. Each subsection below provides a detailed discussion of the themes, their sub-themes, and the corresponding codes for each device. An overview of themes, sub-themes, and codes can be seen in Table 1.

4.1. Technical challenges

This theme includes four sub-themes: *digital forensics workflow*, *forensic tool challenges*, *technological evolution*, and *evidence acquisition.*

[1] A sample of the coding can be found in Table 2

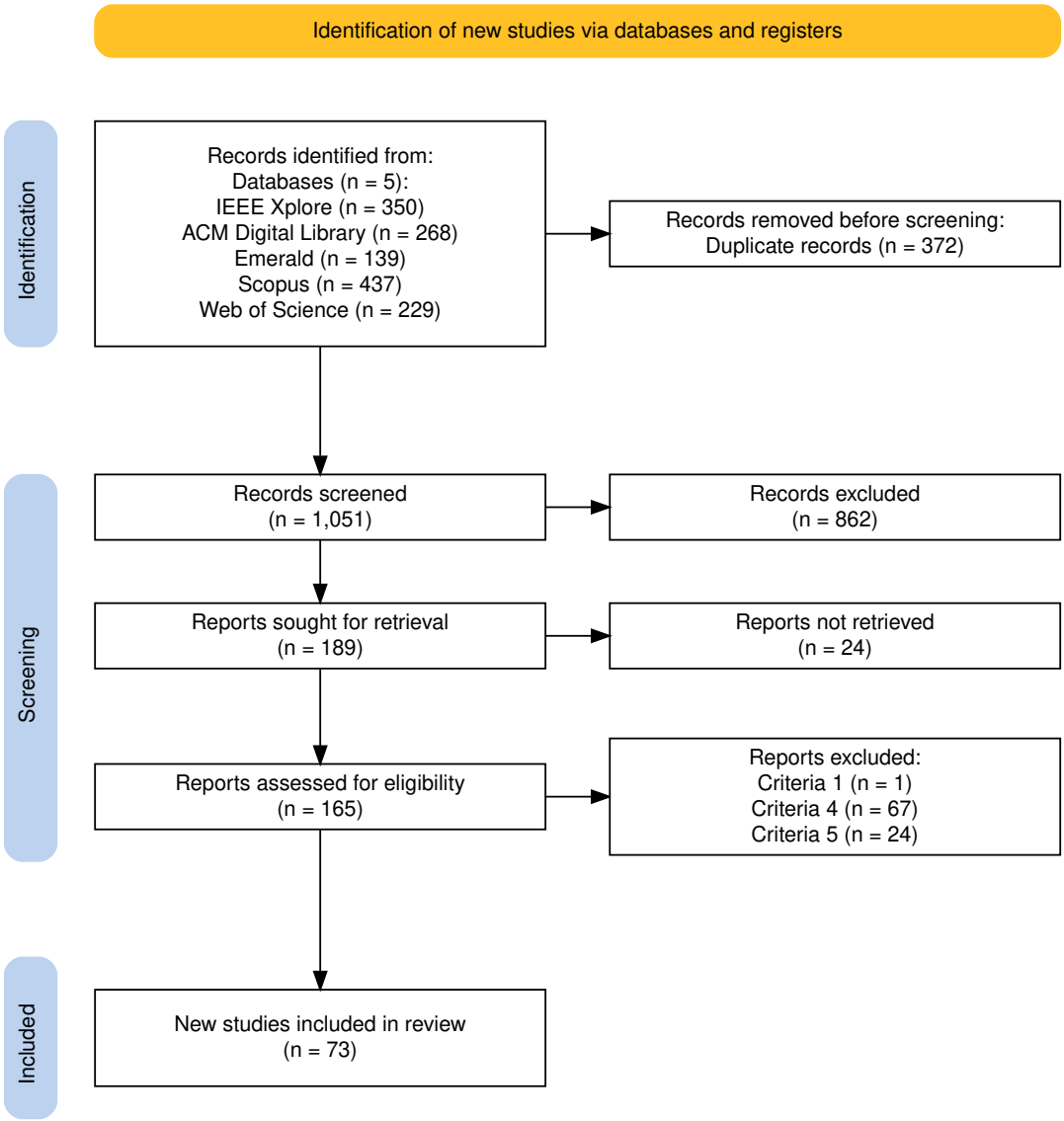

Figure 1: PRISMA flow chart outlining search and screening process based on Haddaway et al. [44]

4.1.1. Smartphones

The first sub-theme, *digital forensics workflow*, concerns challenges related to the forensic process itself—whether due to the vast volume of data or the fact that devices under investigation may still be active and continue to generate data. Eight codes were identified. *Rooting/jailbreaking* refers to obtaining elevated permissions on a device to enable physical acquisition, which can enhance evidence recovery. However, this process introduces risks, such as compromising the device's integrity or causing data loss [45, 46]. When rooting or jailbreaking is not possible, important artefacts may remain unrecovered, and physical acquisition becomes infeasible [47, 48]. Another issue is *cloud data*, which presents acquisition difficulties due to its distributed nature and the sheer volume of data typical of cloud-linked smartphone storage [49, 50].

The *size of data* itself presents analytical challenges, as investigators must manage and interpret large, diverse datasets [10, 51, 48, 52]. Relatedly, difficulties arise from *foreign apps and languages*, which can introduce delays and risks of misinterpretation [53, 52]. *Physical acquisition* methods are also challenged by their cost, complexity, and time demands [45].

Moreover, traditional *post-mortem analysis* approaches are often unsuitable due to the real-time and interactive nature of smartphones [54]. Finally, *data interpretation* remains a core difficulty, as

Table 1
Themes, sub-themes, and codes for smartphones and smartwatches—where * and ** indicates codes or sub-themes specific to smartphones and smartwatches, respectively.

Theme	Sub-theme	Code(s)
Technical challenges	Digital forensics workflow	Rooting/jailbreaking*, Cloud data*, Size of data*, foreign apps and languages*, physical acquisition*, post-mortem analysis limitations*, data interpretation*, syncing device with the cloud**, live devices**
	Forensic tool challenges	Tool limitations, tool reliability*, lack of tools*, special tools*, incomplete data recovery*
	Technological evolution	device infrastructure fragmentation, ever evolving technology,
	Evidence acquisition	Troubles accessing certain data*, difference between rooted and unrooted*, reliability issues for evidences*, volatile evidence, evidence damaged*, login activities*, user-controlled data limitations*
Anti-forensics challenges	Data protection and anti-forensics	Encryption, anti-forensic techniques and data wiping*
	Security*	Authentication*, security features*
Methodological and development challenges	Method	lack of standardisation*, linking data to real identities*, inadequate methods*, no standard for wearable tech**,
	Development constraints*	Vocabulary limitations*, limited sample number*
	Research constraints**	Lack of research**, finding datasets**
Legal challenges	n/a	Legal issues

investigators must navigate diverse formats and artefacts across apps and systems [55, 52].

The second sub-theme, *forensic tool challenges*, focuses on limitations of the tools employed in mobile forensics. *Tool limitations* are prominent, particularly when tools lack support for certain artefacts, operating systems, or applications [56, 45, 10, 57, 53, 58, 59, 47, 60, 61, 62, 63]. High costs and system requirements can further restrict tool accessibility [51].

Tool reliability also poses a concern due to inconsistent performance in evidence recovery and common issues such as slow updates, bugs, and ineffective filtering [10, 64, 65, 66, 51, 67, 46, 53]. In addition, investigators often face a *lack of tools* suited for handling large datasets or specialised scenarios [49, 52]. Some tasks require *special tools*, particularly for physical extractions, which allow for more comprehensive data retrieval [51]. Nonetheless, even with advanced tools, *incomplete data recovery* may occur, resulting in loss of critical artefacts [68].

The third sub-theme, *technological evolution*, relates to the pace of technological change and its implications for forensic practice. *Device infrastructure fragmentation* poses significant challenges, as investigators must contend with a variety of operating systems [56, 49, 57, 55], hardware platforms, and proprietary software structures [45]. This includes difficulties linked to unique file systems [69], data discrepancies across services [70], and the fragmentation of device models and manufacturers [71, 72, 9, 73, 74, 75]. Keeping up with evolving services further adds to this burden [76].

Ever evolving technology amplifies this challenge by making it difficult to ensure that forensic tools and methods remain compatible with emerging technologies [45, 49, 50, 72, 9, 77, 65, 78, 63, 79, 73].

The final sub-theme under *technical challenges* is *evidence acquisition*, consisting of seven codes. *Troubles accessing certain data* include obstacles in retrieving specific data stored on mobile devices [45, 75]. A related issue is the *difference between rooted and unrooted* devices, which affects the volume

and type of data that can be accessed [80, 81, 82, 83, 84, 85, 86, 87, 88, 89]. Unlike the earlier discussion about rooting that focused on gaining elevated privileges through rooting, this relates to the practical effects for data extraction—specifically, how the device's rooted status determines the types and volume of data that forensic tools can retrieve.

The complexity of digital data also introduces *reliability issues for evidences*, where artefacts may be misinterpreted or lack verifiable accuracy [90, 91]. Another challenge is the presence of *volatile evidence*, which is vulnerable to loss or alteration if not captured promptly [49, 76, 92, 55, 93, 94, 81]. In some instances, *evidence may be damaged* during acquisition, further impacting evidentiary completeness [64].

Login activities are also difficult to identify and confirm, making it challenging to attribute actions to specific users [76]. Lastly, *user-controlled data limitations* reflect the risks associated with users deleting, modifying, or encrypting their data before or during forensic procedures [74].

4.1.2. Smartwatches

The first sub-theme, *digital forensics workflow*, includes challenges associated with the dynamic nature of smartwatches and their integration with external systems. One issue is *syncing device with the cloud*, where syncing Fitbit devices with cloud services at specific times complicated the forensic analysis by introducing inconsistencies in the data timeline [40]. Additionally, the challenge of *live devices* arises when devices remain active during the investigation, potentially continuing to collect data and thereby compromising the integrity of the evidence [40].

The next sub-theme, *forensic tool challenges*, relates to the limitations of tools employed in smartwatch investigations. *Tool limitations* were noted where commercial and traditional forensic tools failed to access all storage locations or accurately recover and decode artefacts from smartwatches [95]. Furthermore, these tools may lack support for certain data types or process data incorrectly, reducing the reliability and completeness of the extracted evidence [96].

The third sub-theme, *technological evolution*, reflects how the rapid pace and diversity of consumer electronics complicate forensic practices. *Device infrastructure fragmentation* makes it difficult to conduct comprehensive research or develop tools compatible with the wide array of available smartwatch models [73]. Adding to this, the issue of *ever evolving technology* highlights the ongoing need for forensic investigators to continuously update their knowledge and adapt to newly introduced technologies [40].

The fourth and final sub-theme, *evidence acquisition*, focuses on the limited accessibility and temporal nature of certain types of smartwatch data. *Volatile evidence* was identified as a major challenge, with some data being retained for only short periods—such as 13 to 15 days—before it becomes permanently inaccessible, thereby narrowing the window of opportunity for successful evidence collection [96].

4.2. Anti-forensic challenges

This theme entails obstacles that hinder the collection and analysis of digital evidence. For smartphones, this theme includes two sub-themes: *data protection and anti-forensics* and *security*, which cover challenges such as encryption, data wiping, and various anti-forensic techniques. For smartwatches, the theme similarly addresses these obstacles but includes only the sub-theme *data protection and anti-forensics*.

4.2.1. Smartphones

The first sub-theme, *data protection and anti-forensics*, addresses deliberate or systemic obstacles to forensic investigations. A key challenge is *encryption*, where encrypted files and data render information unreadable or inaccessible to both investigators and forensic tools [45, 10, 49, 54, 97, 66, 98, 48, 89, 99, 55, 79, 46, 100, 101]. This challenge highlights the need for forensic tools capable of decrypting protected content [53]. Closely related are *anti-forensics techniques and data wiping*, which refer to the deliberate use of apps or tools to delete, conceal, or alter data to obstruct investigations [45, 102, 10, 49, 7, 103, 92, 97, 72, 66, 86, 104, 88, 105, 74]. These activities require effective countermeasures [53]. Additionally,

foreign applications may be used as anti-forensic tools, introducing further complexity [52], while some suspects employ anti-reverse engineering techniques to prevent forensic analysis [106].

The second sub-theme, *security*, includes device-level and software-level protective mechanisms that hinder forensic access. The first issue, *authentication*, involves access barriers such as PINs and passcodes that prevent entry into devices [45, 72, 69]. Many Android devices, in particular, feature lock screens that remain resistant to current forensic techniques, requiring the development of improved access methods [53, 74]. The second issue, *security features*, refers to embedded protections at the device or application level that restrict access to data. These include security protocols, app-level restrictions, and regular security updates that can interfere with evidence retrieval efforts [49, 54, 97, 9, 99, 98, 84].

4.2.2. Smartwatches

The sub-theme *data protection and anti-forensics* focuses on challenges that hinder forensic investigation, often unintentionally, such as encryption, which protects user privacy but can also conceal evidence. Within this sub-theme, the code *encryption* was identified, referring to difficulties in accessing information stored in encrypted files [107] or data rendered inaccessible due to encryption [108, 6].

4.3. Methodological and development challenges

The theme *methodological and development challenges* includes two sub-themes related to the approaches and limitations in forensic investigation. For smartphones, these sub-themes are *method* and *development constraints*, addressing challenges such as the lack of standardisation across operating systems, file formats, and the difficulties in developing new methods or tools. For smartwatches, the sub-themes are *method* and *research constraints*, focusing on challenges in the methods applied specifically to smartwatches as well as broader research and development limitations within the field.

4.3.1. Smartphones

The first sub-theme, *method*, includes various methodological challenges in smartphone forensics. One major issue is the *lack of standardisation*, which arises from the absence of a unified forensic approach that extends beyond the operating system level [56]. This includes the limited availability of techniques supporting diverse platforms [10], the lack of standardised data collection procedures [7], and the absence of consistent forensic file formats [53]. Another methodological concern is *linking data to real identities*, which reflects the difficulty of associating digital artefacts with the actual perpetrators of a crime. Furthermore, the use of *inadequate methods* presents technical obstacles, such as synchronisation issues between metadata and flash storage during the data acquisition process [56].

The second sub-theme, *development constraints*, focuses on challenges affecting the advancement of forensic tools and techniques. *Vocabulary limitations* hinder the accuracy of classification tasks due to a restricted word set, which limits the system's ability to distinguish between relevant and irrelevant data [109]. Similarly, a *limited sample number* undermines the performance of forensic algorithms, particularly when only a small number of vault applications are available for analysis [110].

4.3.2. Smartwatches

The first sub-theme, *method*, identifies the absence of established procedures as a core limitation in smartwatch forensics. Specifically, the code *no standard for wearable tech* reflects the lack of a recognised framework for conducting investigations on wearable devices. This creates difficulties for investigators in locating and analysing all relevant data, which can compromise the accuracy and integrity of findings [40].

The second sub-theme, *research constraints*, relates to limitations in the current state of forensic research on smartwatches. One challenge is the *lack of research*, as many widely used smartwatch models have not yet been thoroughly examined, increasing the likelihood that relevant artefacts remain

unidentified [81]. A related issue is *finding datasets*, which refers to the difficulty in accessing extended datasets that reflect real-world usage patterns—essential for validating forensic techniques [111].

4.4. Legal challenges

The fourth and final theme, *legal challenges*, relates to laws and regulations that may restrict investigators' ability to access or utilize certain information. As only a single code, *legal issues*, was identified, no sub-themes were formed under this theme for either smartphones or smartwatches.

4.4.1. Smartphones

The code *legal issues* highlights the legal complexities involved in smartphone forensics. Information retrieved from smartphones is often highly sensitive and potentially admissible in court; however, its use is governed by strict legal frameworks designed to protect user privacy [49]. Additional difficulties arise due to the evolving nature of corporate policies that determine how, and under what conditions, digital evidence may be shared with law enforcement agencies [9]. Furthermore, accessing specific user information often requires formal legal procedures, such as obtaining subpoenas from Internet Service Providers (ISPs), which can delay investigations [58].

4.4.2. Smartwatches

The same code *legal issues*, also applies to smartwatch forensics. A key issue concerns the time-consuming process of data retrieval from user accounts. Although it is technically possible to download archived data, the steps involved in verifying legal requests and receiving the requested information from service providers can take several weeks or even months, thereby delaying the timeliness of forensic investigations [40].

5. Discussion

The challenges identified in this study align with previous reviews on mobile forensics. Sharma et al. [74] highlights obstacles such as lock screen authentication and remote data wiping after device seizure, while Fukami et al. [97] underscores encryption, data wiping, and security features as major barriers. This study confirms these persistent challenges, including the complexity posed by diverse smartphone models [74], and adds further issues related to legal constraints and tool limitations. For smartwatches, the lack of forensic research corresponds with observations by Rightley and Karabiyik [81] and Al-Sharrah et al. [22]. Unlike prior work, this review uniquely integrates challenges across both smartphones and smartwatches, revealing smartwatch-specific issues not previously reported.

This study focuses on the socio-technical side, highlighting how technology and social values work together and impact society. For example, encryption emerges as a major challenge for forensic investigations across both smartphones and smartwatches. While encryption prevents forensic investigators from accessing potentially crucial evidence—thus potentially enabling criminal activity to go undetected—it simultaneously serves a critical function for everyday users seeking to protect their privacy and secure sensitive information, as well as being a default setting on many devices and services used in a modern digital society.

This paradox reveals the socio-technical complexity of encryption challenges in digital forensics, where efforts to overcome such challenges may both strengthen legal processes and contribute to positive societal outcomes. Therefore, while this study aims to contribute valuable insights into current forensic challenges, it also acknowledges the broader social trade-offs involved, particularly concerning individuals' digital rights and privacy in an increasingly interconnected world.

6. Conclusion and limitations

This study aimed to identify current challenges in digital forensic analysis of smartphones and smartwatches and answer the question: "*How do the challenges in forensic analysis differ between smartphones and smartwatches?*" A systematic literature review was conducted, analysing 73 articles from five databases through thematic coding.

The results showed significantly more challenges identified for smartphones than for smartwatches. This suggests that smartphone forensics presents a broader and more discussed set of challenges. Two hypotheses explain this difference: (H_1) smartphones are inherently more complex, or (H_2) there is less research on smartwatches, so many challenges remain unidentified. The second, H_2, is more likely given the difference in the amount of published articles. Some challenges are device-specific—such as *finding datasets* for smartwatches—while others like *authentication* appear for smartphones but were not identified for smartwatches, possibly due to less secure lock screens or less research focus.

Limitations include terminology overlap—terms like smartwatches, fitness trackers, wearables, and IoT were sometimes used interchangeably in the literature, which may have led to missing relevant studies. Future searches could refine terms to improve coverage.

6.1. Smartphones

Thematic coding for smartphones revealed four main themes and eight sub-themes. The most frequent codes were *anti-forensic techniques and data wiping (20)* and *encryption (16)*. Smartphones had 36 identified challenges, more than triple the 11 challenges found for smartwatches. Some challenges, such as bypassing PIN codes, were expected to appear for smartwatches but did not, again pointing to possible research gaps. Smartphones also had more published studies, reflecting greater research attention.

6.2. Smartwatches

For smartwatches, seven sub-themes emerged, with *encryption (3)* and *tool limitations (2)* as the most mentioned challenges. The smaller number of challenges corresponds with fewer published articles. Device-specific challenges for smartwatches included *no standard for wearable tech* and *lack of research*, underscoring the early stage of smartwatch forensics. Encryption was a shared challenge for both devices. As research progresses, smartwatches will likely present new, unique challenges requiring tailored forensic methods.

7. Future research

Smartwatch forensics is under-researched, as shown by the small number of identified challenges and articles. Future studies should include additional databases to capture more comprehensive challenges, especially for smartwatches. Clarifying terminology around smartwatches, fitness trackers, and wearables will also aid research clarity. Since encryption remains the most cited challenge, further efforts should focus on overcoming this barrier to evidence access.

This research is vital for forensic investigators aiming to collect more evidence and solve more crimes. As society digitizes, the importance of addressing digital forensic challenges will only grow.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT-4 and Grammarly in order to check grammar and spelling. After using these tools, the authors reviewed and edited the content as needed and takes full responsibility for the publication's content.

References

[1] N. A. Aziz, M. A. Bin Noor Azmi, M. H. Bin Ahmad Rumaizi, Acquiring Digital Evidence from Health and Safety Devices, in: 2023 IEEE International Conference on Computing (ICOCO), 2023, pp. 311–316. doi:10.1109/ICOCO59262.2023.10397678.

[2] BBC News, *Greece killing: Husband confesses to Caroline Crouch death*, 2021. Retrieved February 24, 2025, from https://www.bbc.com/news/world-europe-57523469.

[3] L. Laricchia, *Smartwatches - Statistics & Facts*, Statista, 2024. Retrieved February 28, 2025, from https://www.statista.com/topics/4762/smartwatches/#topicOverview.

[4] N. Kumar, *Smartwatch Statistics (2025): Market & Sales Data*, DemandSage, 2024. Retrieved February 28, 2025, from https://www.demandsage.com/smartwatch-statistics/.

[5] P. Pawar, *Smartwatch statistics by vendors, revenue and number of users*, Electro IQ, 2024. Retrieved February 28, 2025, from https://electroiq.com/stats/smartwatch-statistics/.

[6] M. Kim, Y. Shin, W. Jo, T. Shon, Security Analysis of Smart Watch and Band Devices, in: 2021 International Conference on Computational Science and Computational Intelligence (CSCI), 2021, pp. 655–658. doi:10.1109/CSCI54926.2021.00172.

[7] B. K. Sharma, M. Walia, Y. Sharma, M. A. Beig, V. Shukla, Advances and Challenges in Mobile Phone Forensics, in: 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), 2024, pp. 1880–1886. doi:10.1109/IC3SE62002.2024.10592965.

[8] S. Kemp, *The Global State of Digital in 2024*, Datareportal, 2024. Retrieved February 28, 2025, from https://datareportal.com/reports/digital-2024-october-global-statshot.

[9] H. Alatawi, K. Alenazi, S. Alshehri, S. Alshamakhi, M. Mustafa, A. Aljaedi, Mobile Forensics: A Review, in: 2020 International Conference on Computing and Information Technology (ICCIT-1441), 2020, pp. 1–6. doi:10.1109/ICCIT-144147971.2020.9213739.

[10] A. Aljahdali, N. Alsaidi, M. Alsafri, A. Alsulami, T. Almutairi, Mobile device forensics, Revista Română de Informatică și Automatică 31 (2021) 81–96. doi:10.33436/v31i3y202107.

[11] B. Kitchenham, S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report EBSE-2007-01, Evidence-Based Software Engineering (EBSE), 2007.

[12] G. Paré, S. Kitsiou, Chapter 9 Methods for Literature Reviews, in: Handbook of eHealth Evaluation: An Evidence-based Approach [Internet], University of Victoria, 2017.

[13] V. Braun, V. Clarke, Using thematic analysis in psychology, Qualitative Research in Psychology 3 (2006) 77–101. doi:10.1191/1478088706qp063oa.

[14] S. Dogan, E. Akbal, Analysis of mobile phones in digital forensics, in: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017, pp. 1241–1244. doi:10.23919/MIPRO.2017.7973613.

[15] S. Rasnayaka, T. Sim, Your Tattletale Gait Privacy Invasiveness of IMU Gait Data, in: 2020 IEEE International Joint Conference on Biometrics (IJCB), 2020, pp. 1–10. doi:10.1109/IJCB48548.2020.9304922.

[16] P. Delgado-Santos, G. Stragapede, R. Tolosana, R. Guest, F. Deravi, R. Vera-Rodriguez, A Survey of Privacy Vulnerabilities of Mobile Device Sensors, ACM Comput. Surv. 54 (2022) 224:1–224:30. doi:10.1145/3510579.

[17] N. Yodpijit, N. Tavichaiyuth, M. Jongprasithporn, C. Songwongamarit, T. Sittiwanchai, The use of smartphone for gait analysis, in: 2017 3rd International Conference on Control, Automation and Robotics (ICCAR), 2017, pp. 543–546. doi:10.1109/ICCAR.2017.7942756.

[18] S. K. Al Kork, I. Gowthami, X. Savatier, T. Beyrouthy, J. A. Korbane, S. Roshdi, Biometric database for human gait recognition using wearable sensors and a smartphone, in: 2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART), 2017, pp. 1–4. doi:10.1109/BIOSMART.2017.8095329.

[19] D. Ghosh, S. Roy, U. Roy, D. D. Sinha, Gait Identity Verification Using Equipped Smartphone Sensors, in: 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 2020, pp. 1–3. doi:10.1109/NCETSTEA48365.2020.9119955.

[20] A. Mailangkay, Determinants of user satisfaction on interest of smartwatch usage after covid-19, in: 2023 International Conference on Information Management and Technology (ICIMTech), 2023, pp. 517–522. doi:10.1109/ICIMTech59029.2023.10277879.

[21] M. E. Cecchinato, A. L. Cox, Smartwatches: Digital handcuffs or magic bracelets?, Computer 50 (2017) 106–109. doi:10.1109/MC.2017.117.

[22] M. Al-Sharrah, A. Salman, I. Ahmad, Watch Your Smartwatch, in: 2018 International Conference on Computing Sciences and Engineering (ICCSE), 2018, pp. 1–5. doi:10.1109/ICCSE1.2018.8374228.

[23] N. R. Odom, J. M. Lindmar, J. Hirt, J. Brunty, Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices, Journal of Forensic Sciences 64 (2019) 1673–1686. doi:10.1111/1556-4029.14109.

[24] S. Becirovic, S. Mrdovic, Manual IoT Forensics of a Samsung Gear S3 Frontier Smartwatch, in: 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2019, pp. 1–5. doi:10.23919/SOFTCOM.2019.8903845.

[25] M. Harbawi, A. Varol, The role of digital forensics in combating cybercrimes, in: 2016 4th International Symposium on Digital Forensic and Security (ISDFS), 2016, pp. 138–142. doi:10.1109/ISDFS.2016.7473532.

[26] D. Quick, K.-K. R. Choo, IoT Device Forensics and Data Reduction, IEEE Access 6 (2018) 47566–47574. doi:10.1109/ACCESS.2018.2867466.

[27] A. H. Johnston, G. M. Weiss, Smartwatch-based biometric gait recognition, in: 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2015, pp. 1–6. doi:10.1109/BTAS.2015.7358794.

[28] N. H. AL-Naffakh, Activity-Based User Authentication Using Smartwatches, School of Engineering, Computing and Mathematics Theses (2020). Retrieved April 23, 2025, from https://pearl.plymouth.ac.uk/secam-theses/193.

[29] R. Randombage, N. Jayawardene, Smartwatch-Based Gait Authentication Using Siamese LSTM Networks, in: 2024 9th International Conference on Information Technology Research (ICITR), 2024, pp. 1–5. doi:10.1109/ICITR64794.2024.10857751.

[30] K. Salehzadeh Niksirat, L. Velykoivanenko, N. Zufferey, M. Cherubini, K. Huguenin, M. Humbert, Wearable Activity Trackers: A Survey on Utility, Privacy, and Security, ACM Comput. Surv. 56 (2024) 183:1–183:40. doi:10.1145/3645091.

[31] M. Snyder, *Police: Woman's Fitness Watch Disproved Rape Report*, ABC27 News, 2015. Retrieved February 24, 2025, from https://www.abc27.com/news/police-womans-fitness-watch-disproved-rape-report/.

[32] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E. K. Markakis, A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues, IEEE Communications Surveys & Tutorials 22 (2020) 1191–1221. doi:10.1109/COMST.2019.2962586.

[33] A. Mylonas, V. Meletiadis, L. Mitrou, D. Gritzalis, Smartphone sensor data as digital evidence, Computers & Security 38 (2013) 51–75. doi:10.1016/j.cose.2013.03.007.

[34] I. Bouchrika, M. Goffredo, J. Carter, M. Nixon, On Using Gait in Forensic Biometrics, Journal of Forensic Sciences 56 (2011) 882–889. doi:10.1111/j.1556-4029.2011.01793.x.

[35] J. Ingemarsson, M. Birath, J. Kävrestad, Factors influencing Swedish citizens' willingness to provide their mobile phones to forensic examination, International Journal of Information Security 24 (2024) 42. doi:10.1007/s10207-024-00955-4.

[36] J. Kävrestad, M. Birath, N. Clarke, Fundamentals of Digital Forensics: A Guide to Theory, Springer International Publishing, 2024. doi:10.1007/978-3-031-53649-6.

[37] S. Amiroon, C. Fachkha, Digital Forensics and Investigations of the Internet of Things: A Short Survey, in: 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), 2020, pp. 1–4. doi:10.1109/ICSPIS51252.2020.9340150.

[38] I. Baggili, J. Oduro, K. Anthony, F. Breitinger, G. McGee, Watch What You Wear: Preliminary Forensic Analysis of Smart Watches, in: 2015 10th International Conference on Availability, Reliability and Security, 2015, pp. 303–311. doi:10.1109/ARES.2015.39.

[39] A. Flaglien, I. M. Sunde, A. Dilijonaite, J. Hamm, J. P. Sandvik, P. Bjelland, K. Franke, S. Axelsson, Digital Forensics, John Wiley & Sons, Ltd, 2017. doi:10.1002/9781119262442.

[40] A. Almogbil, A. Alghofaili, C. Deane, T. Leschke, A. Almogbil, A. Alghofaili, Digital Forensic Analysis of Fitbit Wearable Technology: An Investigator's Guide, in: 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2020, pp. 44–49. doi:10.1109/CSCloud-EdgeCom49738.2020.00017.

[41] S. Alabdulsalam, K. Schaefer, T. Kechadi, N.-A. Le-Khac, Internet of Things Forensics – Challenges and a Case Study, in: Advances in Digital Forensics XIV, Springer, Cham, 2018, pp. 35–48. doi:10.1007/978-3-319-99277-8_3.

[42] S. Zawoad, R. Hasan, FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things, in: 2015 IEEE International Conference on Services Computing, 2015, pp. 279–284. doi:10.1109/SCC.2015.46.

[43] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, D. Moher, The prisma 2020 statement: an updated guideline for reporting systematic reviews, BMJ 372 (2021). doi:10.1136/bmj.n71.

[44] N. R. Haddaway, M. J. Page, C. C. Pritchard, L. A. McGuinness, PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis, Campbell Systematic Reviews 18 (2022) e1230. doi:10.1002/cl2.1230.

[45] A. Alblooshi, N. Aljneibi, F. Iqbal, R. Ikuesan, M. Badra, Z. Khalid, Smartphone forensics: A comparative study of common mobile phone models, in: 2024 12th International Symposium on Digital Forensics and Security (ISDFS), 2024, pp. 1–6. doi:10.1109/ISDFS60797.2024.10527262.

[46] T. Hermawan, Y. Suryanto, F. Alief, L. Roselina, Android forensic tools analysis for unsend chat on social media, in: 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2020, pp. 233–238. doi:10.1109/ISRITI51436.2020.9315364.

[47] R. Bardhan, R. Garay-Paravisini, G. Dorai, L. Vanputte, Digital forensics analysis of a financial mobile application: Uncovering security and privacy implications, in: 2024 International Symposium on Networks, Computers and Communications (ISNCC), 2024, pp. 1–8. doi:10.1109/ISNCC62547.2024.10758975.

[48] R. F. Abu Hweidi, M. Jazzar, A. Eleyan, T. Bejaoui, Forensics investigation on social media apps and web apps messaging in android smartphone, in: 2023 International Conference on Smart Applications, Communications and Networking (SmartNets), 2023, pp. 1–7. doi:10.1109/SmartNets58706.2023.10216267.

[49] A. Almuqren, H. Alsuwaelim, M. Hafizur Rahman, A. Ibrahim, A Systematic Literature Review on Digital Forensic Investigation on Android Devices, in: Procedia Computer Science, volume 235, 2024, pp. 1332–1352. doi:10.1016/j.procs.2024.04.126.

[50] F. E. Salamh, M. M. Mirza, S. Hutchinson, Y. H. Yoon, U. Karabiyik, What's on the horizon? an in-depth forensic analysis of android and ios applications, IEEE Access 9 (2021) 99421–99454. doi:10.1109/ACCESS.2021.3095562.

[51] O. Parhad, V. Naik, Comparative analysis of Data Extraction for Qualcomm based android devices, in: 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2023, pp. 1–7. doi:10.1109/ICCCNT56998.2023.10307241.

[52] AL. Zhang, Contextualising the investigation work in China: The facilitators and barriers in using mobile phone evidence, POLICING & SOCIETY 35 (2025) 68–84. doi:10.1080/10439463.2024.2372351.

[53] P. Goncalves, A. Attenberger, H. Baier, Smartphone data distributions and requirements for realistic mobile device forensic corpora, IFIP Advances in Information and Communication Technology 653 IFIP (2022) 47–63. doi:10.1007/978-3-031-10078-9_3.

[54] R. Cuomo, D. D'Agostino, M. Ianulardo, Mobile forensics: Repeatable and non-repeatable technical assessments, Sensors 22 (2022). doi:10.3390/s22187096.

[55] S. M. Arıkan, Ö. Yürekten, Development and maintenance of mobile forensic investigation software modules, in: 2021 9th International Symposium on Digital Forensics and Security (ISDFS), 2021, pp. 1–6. doi:10.1109/ISDFS52919.2021.9486353.

[56] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, K. Siddique, A review of mobile forensic investigation process models, IEEE Access 8 (2020) 173359–173375. doi:10.1109/ACCESS.2020.3014615.

[57] F. Alief, Y. Suryanto, L. Rosselina, T. Hermawan, Analysis of autopsy mobile forensic tools against unsent messages on whatsapp messaging application, in: 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), 2020, pp. 26–30. doi:10.23919/EECSI50503.2020.9251876.

[58] M. M. Mirza, U. Karabiyik, Enhancing ip address geocoding, geolocating and visualization for digital forensics, in: 2021 International Symposium on Networks, Computers and Communications (ISNCC), 2021, pp. 1–7. doi:10.1109/ISNCC52172.2021.9615668.

[59] M. Surya, J. Sidabutar, N. Qomariasih, Comparative analysis of recovery tools for digital forensic evidence using nist framework 800-101 r1, in: 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), 2023, pp. 258–262. doi:10.1109/ICoCICs58778.2023.10276447.

[60] Herman, I. Riadi, I. A. Rafiq, Forensic mobile analysis on social media using national institute standard of technology method, International Journal of Safety and Security Engineering 12 (2022) 707–713. doi:10.18280/ijsse.120606.

[61] I. Riadi, Herman, N. H. Siregar, Mobile forensic analysis of signal messenger application on android using digital forensic research workshop (dfrws) framework, Ingenierie des Systemes d'Information 27 (2022) 903–913. doi:10.18280/ISI.270606.

[62] G. B. Satrya, F. Kurniawan, A novel android memory forensics for discovering remnant data, International Journal on Advanced Science, Engineering and Information Technology 10 (2020) 1008–1015. doi:10.18517/ijaseit.10.3.9363.

[63] M. Stanković, U. Karabiyik, Exploratory study on kali nethunter lite: A digital forensics approach, Journal of Cybersecurity and Privacy 2 (2022) 750–763. doi:10.3390/jcp2030038.

[64] Sunardi, Herman, S. R. Ardiningtias, A comparative analysis of digital forensic investigation tools on facebook messenger applications, Journal of Cyber Security and Mobility 11 (2022) 655–672. doi:10.13052/jcsm2245-1439.1151.

[65] M. M. Mirza, S. Hutchinson, R. Gee, U. Karabiyik, No filters: A deep dive into photo sharing apps on android and ios, in: 2023 International Symposium on Networks, Computers and Communications (ISNCC), 2023, pp. 1–8. doi:10.1109/ISNCC58260.2023.10323868.

[66] A. Menahil, W. Iqbal, M. Iftikhar, W. B. Shahid, K. Mansoor, S. Rubab, Forensic analysis of social networking applications on an android smartphone, Wireless Communications and Mobile Computing 2021 (2021). doi:10.1155/2021/5567592.

[67] I. Riadi, A. Yudhana, G. P. Inngam Fanani, Mobile forensic tools for digital crime investigation: Comparison and evaluation, International Journal of Safety and Security Engineering 13 (2023) 11–19. doi:10.18280/ijsse.130102.

[68] S. Hutchinson, N. Shantaram, U. Karabiyik, Forensic analysis of dating applications on android and ios devices, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 836–847. doi:10.1109/TrustCom50675.2020.00113.

[69] I. Kara, Digital Forensic Analysis of Discord Mobile Application on Android Based Smartphones, ACTA INFOLOGICA 6 (2022) 189–198. doi:10.26650/acin.1109682.

[70] C. Femi-Adeyinka, N. A. Kose, T. Akinsowon, C. Varol, Digital forensics analysis of youtube, instagram, and tiktok on android devices: A comparative study, in: 2024 12th International Symposium on Digital Forensics and Security (ISDFS), 2024, pp. 1–6. doi:10.1109/ISDFS60797.2024.10527244.

[71] A. M. Da Costa, A. O. De Sà, R. C. S. Machado, Data acquisition and extraction on mobile devices-a review, in: 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT), 2022, pp. 294–299. doi:10.1109/MetroInd4.0IoT54413.2022.9831724.

[72] H. A. Hosani, M. Yousef, S. A. Shouq, F. Iqbal, State of the art in digital forensics for small scale digital devices, in: 2020 11th International Conference on Information and Communication Systems (ICICS), 2020, pp. 072–078. doi:10.1109/ICICS49469.2020.239531.

[73] J. P. van Zandwijk, A. Boztas, Digital traces and physical activities: opportunities, challenges and pitfalls, Science and Justice 63 (2023) 369–375. doi:10.1016/j.scijus.2023.04.002.

[74] Y. K. Sharma, S. S. Noval, A. Jain, B. Sabitha, T. Ramya, Forensics-as-a-service: A Review of Mobile Forensics, in: 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022, pp. 486–491. doi:10.1109/IC3I56241.2022.10072726.

[75] Y. Keim, Y. H. Yoon, U. Karabiyik, Digital forensics analysis of ubuntu touch on pinephone, Electronics (Switzerland) 10 (2021) 1–24. doi:10.3390/electronics10030343.

[76] L. Bortnik, A. Lavrenovs, Android dumpsys analysis to indicate driver distraction, Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST 351 (2021) 139–163. doi:10.1007/978-3-030-68734-2_8.

[77] P. Liwen, Image captioning-based smart phone forensics analysis model, in: Proceedings of the 2023 6th International Conference on Big Data Technologies, ICBDT '23, Association for Computing Machinery, New York, NY, USA, 2023, pp. 372–376. doi:10.1145/3627377.3627435.

[78] R. Sinha, V. Sihag, G. Choudhary, M. Vardhan, P. Singh, Forensic analysis of fitness applications on android, Communications in Computer and Information Science 1544 CCIS (2022) 222–235. doi:10.1007/978-981-16-9576-6_16.

[79] T. Sutikno, Mobile forensics tools and techniques for digital crime investigation: a comprehensive review, International Journal of Informatics and Communication Technology 13 (2024) 321–332. doi:10.11591/ijict.v13i2.pp321-332.

[80] E. Akbal, I. Baloglu, T. Tuncer, S. Dogan, Forensic analysis of bip messenger on android smartphones, Australian Journal of Forensic Sciences 52 (2020) 590–609. doi:10.1080/00450618.2019.1610064.

[81] C. Rightley, U. Karabiyik, Digital Forensic Analysis of AGPTEK Smartwatch Application on Android OS, in: 2023 International Symposium on Networks, Computers and Communications (ISNCC), 2023, pp. 1–8. doi:10.1109/ISNCC58260.2023.10323677.

[82] P. Domingues, R. Nogueira, J. C. Francisco, M. Frade, Post-mortem digital forensic artifacts of tiktok android app, in: Proceedings of the 15th International Conference on Availability, Reliability and Security, ARES '20, Association for Computing Machinery, New York, NY, USA, 2020. doi:10.1145/3407023.3409203.

[83] M. R. Laayu, A. Kurniawan, N. D. W. Cahyani, G. B. Satrya, Comparison of acquisition results on iphone 7 plus (ios 14.8.1) between jailbreaking vs non-jailbreaking device, in: 2022 10th International Conference on Information and Communication Technology, ICoICT 2022, 2022, pp. 402–406. doi:10.1109/ICoICT55009.2022.9914862.

[84] M.-R. Boueiz, Importance of rooting in an android data acquisition, in: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1–4. doi:10.1109/ISDFS49300.2020.9116445.

[85] M. S. Al-Faaruuq, D. F. Priambodo, ios digital evidence comparison of instant messaging apps, in: 2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA), 2022, pp. 83–88. doi:10.1109/ICSINTESA56431.2022.10041620.

[86] N. Adi Wibowo, R. Anindya Wijayanti, A. Amiruddin, T. Yulita, J. Sidabutar, A digital evidence analysis of the twinme application on android based on interpol guidelines for digital forensics laboratories, in: 2024 International Conference on Information Technology and Computing (ICITCOM), 2024, pp. 312–317. doi:10.1109/ICITCOM62788.2024.10762406.

[87] N. Hoang Khoa, P. The Duy, H. Do Hoang, D. Thi Thu Hien, V.-H. Pham, Forensic analysis of tiktok application to seek digital artifacts on android smartphone, in: 2020 RIVF International

Conference on Computing and Communication Technologies (RIVF), 2020, pp. 1–5. doi:10.1109/RIVF48685.2020.9140739.

[88] B. Pribadi, S. Rosdiana, S. Arifin, Digital forensics on facebook messenger application in an android smartphone based on nist sp 800-101 r1 to reveal digital crime cases, in: Procedia Computer Science, volume 216, 2023, pp. 161–167. doi:10.1016/j.procs.2022.12.123.

[89] T. Rasul, R. Latif, N. S. M. Jamail, A computational forensic framework for detection of hidden applications on android, Indonesian Journal of Electrical Engineering and Computer Science 20 (2020) 353–360. doi:10.11591/ijeecs.v20.i1.pp353-360.

[90] C. Berger, B. Meylan, T. R. Souvignet, Uncertainty and error in location traces, Forensic Science International: Digital Investigation 51 (2024). doi:10.1016/j.fsidi.2024.301841.

[91] E. Ryser, H. Spichiger, D.-O. Jaquet-Chiffelle, Geotagging accuracy in smartphone photography, Forensic Science International: Digital Investigation 50 (2024). doi:10.1016/j.fsidi.2024.301813.

[92] E. Dragonas, C. Lambrinoudakis, Forensic analysis of android notifications' history, in: 2024 IEEE International Conference on Cyber Security and Resilience (CSR), 2024, pp. 01–06. doi:10.1109/CSR61664.2024.10679344.

[93] J. P. van Zandwijk, A. Boztas, The phone reveals your motion: Digital traces of walking, driving and other movements on iphones, Forensic Science International: Digital Investigation 37 (2021). doi:10.1016/j.fsidi.2021.301170.

[94] X. Semenova, N. Knyazeva, Forensic analysis of 2gis navigation app installed on an android-based smartphone, in: 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2021, pp. 0459–0462. doi:10.1109/USBEREIT51232.2021.9455059.

[95] L. Dawson, A. Akinbi, Challenges and opportunities for wearable iot forensics: Tomtom spark 3 as a case study, Forensic Science International: Reports 3 (2021). doi:10.1016/j.fsir.2021.100198.

[96] S. Hutchinson, M. M. Mirza, N. West, U. Karabiyik, M. K. Rogers, T. Mukherjee, S. Aggarwal, H. Chung, C. Pettus-Davis, Investigating wearable fitness applications: Data privacy and digital forensics analysis on android, Applied Sciences (Switzerland) 12 (2022). doi:10.3390/app12199747.

[97] A. Fukami, R. Stoykova, Z. Geradts, A new model for forensic data extraction from encrypted mobile devices, Forensic Science International: Digital Investigation 38 (2021) 301169. doi:10.1016/j.fsidi.2021.301169.

[98] M. Park, S. Kim, J. Kim, Research on note-taking apps with security features, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 11 (2020) 63–76. doi:10.22667/JOWUA.2020.12.31.063.

[99] S. K. Chaudhry, J. K. S V, S. K. S, P. V S, Impact of factory reset on android devices, in: 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2023, pp. 1–6. doi:10.1109/ICCCNT56998.2023.10308267.

[100] D. Wijnberg, N.-A. Le-Khac, Identifying interception possibilities for whatsapp communication, Forensic Science International: Digital Investigation 38 (2021). doi:10.1016/j.fsidi.2021.301132.

[101] Y. Gong, U. Karabiyik, Forensics analysis of android social networking application: Tencent qq revisited, in: 2024 International Symposium on Networks, Computers and Communications (ISNCC), 2024, pp. 1–8. doi:10.1109/ISNCC62547.2024.10758981.

[102] A. Akinbi, E. Ojie, Forensic analysis of open-source xmpp/jabber multi-client instant messaging apps on android smartphones, SN Applied Sciences 3 (2021). doi:10.1007/s42452-021-04431-9.

[103] P. Domingues, J. Francisco, M. Frade, Post-mortem digital forensics analysis of the zepp life android application, Forensic Science International: Digital Investigation 45 (2023). doi:10.1016/j.fsidi.2023.301555.

[104] N. F. Mahendra, R. Khairunnisa, Digital forensic analysis of online dating applications on

android using the digital forensic research workshop 2001 investigation model, in: 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), 2023, pp. 218–223. doi:10.1109/ICoCICs58778.2023.10276752.

[105] S. S. Zehra, S. Qadir, Forensic data analysis of delivery and transport applications, in: 2022 International Conference on Cyber Warfare and Security (ICCWS), 2022, pp. 62–68. doi:10.1109/ICCWS56285.2022.9998473.

[106] Y. Zhang, B. Li, Y. Sun, Android encryption database forensic analysis based on static analysis, in: Proceedings of the 4th International Conference on Computer Science and Application Engineering, CSAE '20, Association for Computing Machinery, New York, NY, USA, 2020. doi:10.1145/3424978.3425068.

[107] P. Donaire-Calleja, A. Robles-Gómez, L. Tobarra, R. Pastor-Vargas, Forensic analysis laboratory for sport devices: A practical use case, Electronics (Switzerland) 12 (2023). doi:10.3390/electronics12122710.

[108] M. Kim, Y. Shin, W. Jo, T. Shon, Digital forensic analysis of intelligent and smart iot devices, Journal of Supercomputing 79 (2023) 973–997. doi:10.1007/s11227-022-04639-5.

[109] C. Nwankwo, H. Wimmer, L. Chen, J. Kim, Text classification of digital forensic data, in: 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2020, pp. 0661–0667. doi:10.1109/IEMCON51383.2020.9284913.

[110] N. Xie, H. Bai, R. Sun, X. Di, Android vault application behavior analysis and detection, Communications in Computer and Information Science 1257 CCIS (2020) 428–439. doi:10.1007/978-981-15-7981-3_31.

[111] L. Jennings, M. Sorell, H. G. Espinosa, The provenance of apple health data: A timeline of update history, Forensic Science International: Digital Investigation 50 (2024). doi:10.1016/j.fsidi.2024.301804.

A. Sample of thematic coding

Table 2
Sample from the thematic coding—showcasing how the coding were structured

Author(s)	Code	Text with Sub-theme and Theme
…	…	…
[56]	Tool limitations	*Most of the mobile forensic tools do not support or do not have capabilities that can enable integration of application artifacts with known encodings like PDF or MS-Word.* Sub-theme: Forensic Tool Challenges; Theme: Technical Challenges
[45]	Encryption, authentication	*Furthermore, to secure user data, Windows smartphone devices contain encryption and security features such as device encryption and user authentication. However, these security procedures may obstruct data extraction and analysis throughout the forensic process.* Sub-theme: Data Protection and Anti-Forensics, Security; Theme: Anti-Forensics Challenges
[40]	Ever evolving technology	*With new and innovative technology entering the market every few weeks, digital forensic investigators have to continuously learn and update their current knowledge and skills on how to digitally investigate these devices.* Sub-theme: Technological Evolution; Theme: Technical Challenges
[80]	Difference between rooted and unrooted	*The proposed methodology also shows that there are significant differences between rooted and unrooted devices for data acquisition.* Sub-theme: Evidence acquisition; Theme: Technical Challenges
[97]	Anti-forensic techniques and data wiping	*Also, effective data erasing functions at the OS level make it difficult to find data remnants in physical data.* Sub-theme: Data Protection and Anti-Forensics; Theme: Anti-Forensics Challenges
[7]	Lack of standardisation	*Unfortunately, there is not yet a standardised method for gathering data from these devices that may be relevant to scientists.* Sub-theme: Method; Theme: Methodological and Development Challenges
…	…	…