Integrating NIST SP 800-101 and ISO/IEC 27000 for Mobile Device Forensics: A Conceptual Framework

Stephanie Agenbag[1] [0009-0003-2321-4335], Andre Henney[2] [0000-0003-2447-1555] and Heloise Pieterse[3, 4] [0000-0002-2908-4012]

[1, 2, 3] University of the Western Cape, Robert Sobukwe Road, Bellville, 7535, South Africa
[4] National Integrated Cyberinfrastructure System (NICIS), Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
3844494@myuwc.ac.za

Abstract. Mobile device forensics has become central to digital investigations, yet existing process models for smartphones and other portable devices remain fragmented, platform-specific, and inconsistently aligned with international standards. This paper proposes an integrated conceptual framework for mobile digital forensics that combines the operational phases of NIST SP 800-101 Rev. 1 (Preservation, Acquisition, Examination/Analysis, Reporting) with the governance and validation principles of the ISO/IEC 27000-family standards, including ISO/IEC 27037, 27040, 27041, 27042, 27043, and 27050. The conceptual framework explicitly incorporates contemporary mobile challenges—such as platform diversity, file-system variation, strong encryption, application-centric data storage, high data volatility, and cloud dependencies—and maps them to concrete activities and controls at each phase. The paper illustrates how this integrated model can guide evidence handling, tool validation, and artefact analysis in mobile investigations, addressing long-standing inconsistencies in mobile forensic practice. The proposed conceptual framework aims to support more defensible, repeatable mobile device forensics and to provide a basis for future empirical evaluation and tool-agnostic checklists.

Keywords: Mobile Device Forensics, NIST SP 800-101, ISO/IEC 27000, Digital Evidence, Conceptual Framework, Process Model, Validation.

1 Introduction

Digital forensics is a branch of forensic science concerned with the recovery and investigation of material from digital devices and cybercrime [1]. As digital devices have become pervasive, mobile device forensics has emerged as a vital sub-discipline focused on extracting and interpreting evidence from smartphones and other mobile technologies in support of criminal, civil, and intelligence investigations [2], [3]. Mobile devices, such as Android and iOS smartphones, are particularly significant because they integrate advanced computing capabilities, cellular and wireless connectivity, and a variety of sensors, enabling detailed reconstruction of user behaviour and interactions in a connected environment.

Compared with traditional computer forensics, mobile device forensics must contend with a rapidly shifting and heterogeneous landscape: multiple mobile operating

systems, vendor-specific modifications, evolving file systems, pervasive encryption, application-centric data storage, and deep integration with cloud services. These characteristics create substantial challenges for evidence preservation, acquisition, examination, and reporting, and they place a premium on structured, repeatable, and legally defensible forensic processes [4], [5], [6].

The National Institute of Standards and Technology (NIST) Special Publication 800-101 Rev. 1 provides one of the most widely cited mobile device forensic process models, defining four core phases—Preservation, Acquisition, Examination/Analysis, and Reporting [1]. In parallel, the International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC) 27000 family of standards offers internationally recognised best-practice guidance on digital investigations, evidence handling, analysis, tool validation, and legal defensibility [7], [8], [9], [10]. However, these standards are often applied in isolation, and many published mobile forensic process models do not explicitly integrate NIST's operational workflow with ISO/IEC's governance and assurance principles, nor do they fully account for modern mobile technical constraints.

A range of conceptual frameworks and process models have been proposed to structure mobile device forensic investigations, harmonise terminology, or adapt traditional digital forensic processes to mobile contexts. These include harmonised process models, conceptual metamodels, and mobile-specific frameworks that outline investigative phases or activities. While these efforts have helped clarify the scope and complexity of mobile forensics, they also exhibit recurring limitations.

First, many existing frameworks are conceptual and have limited empirical evaluation across the diversity of modern mobile devices, operating systems, and security configurations. Second, although several models align high-level forensic phases, they often lack explicit and systematic integration with internationally recognised standards, particularly with respect to governance, documentation, and validation requirements. Third, prior frameworks frequently emphasise selected stages of the forensic process—such as acquisition or analysis—without explicitly addressing cross-phase validation or the cumulative impact of contemporary mobile constraints, including strong encryption, application sandboxing, and cloud-integrated data storage.

The framework proposed in this paper is likewise conceptual but differs in its explicit integrative focus. Rather than introducing a new standalone process model, it synthesises the NIST SP 800-101 Rev. 1 operational workflow with complementary ISO/IEC 27000-family standards to clarify how operational activities, governance requirements, and validation considerations relate across all investigation phases. By making these relationships explicit and situating them within the practical constraints of modern mobile platforms, the framework aims to reduce methodological fragmentation and provide a coherent, standards-aligned reference model for future evaluation and operational refinement.

This paper addresses this gap by proposing an integrated, mobile-oriented conceptual forensic process framework that:

- Uses the NIST SP 800-101 Rev. 1 model as the operational backbone for mobile device investigations.
- Embeds relevant ISO/IEC 27000-family standards as governance and validation layers at each phase of the process.

- Instantiates the framework for mobile devices by incorporating platform-specific challenges, artefact categories, and validation needs into the activities associated with each phase.

The remainder of this paper is structured as follows. Section 2 reviews mobile-specific forensic challenges, the NIST SP 800-101 model, ISO/IEC standards relevant to digital forensics, and the fragmentation of existing mobile forensic process models. Section 3 presents the integrated NIST–ISO/IEC conceptual framework tailored to mobile devices. Section 4 illustrates how the framework can be applied in mobile investigations and how it informs tool selection and validation. Section 5 discusses benefits and limitations, and Section 6 concludes with directions for future work.

2 Background and Related Work

2.1 Mobile-specific challenges in device forensics.

Traditional desktop forensic environments are often built around comparatively homogeneous operating systems and well-documented file systems, such as New Technology File System (NTFS) and Fourth Extended File System (EXT4). In contrast, mobile device forensics must operate in a highly diverse ecosystem, most notably between Android and iOS, and further complicated by device manufacturers' customised firmware, modified file system layouts, proprietary partition schemes, and vendor-specific security features [6], [11], [12], [13]. This fragmentation leads to differences in where and how data is stored, which artefacts are accessible, and how forensic tools must be configured to extract and interpret potential evidence [11], [13], [14], [15].

On mobile devices, file systems and storage formats have evolved significantly. Modern Android devices, for example, have moved from legacy Yet Another Flash File System 2 (YAFFS2) to primarily using EXT4 and Flash Friendly File System (F2FS), along with specific storage practices and data formats [16], [17], [18]. Similarly, Apple's iOS platform has evolved from the Hierarchical File System Plus (HFS+), which offered limited user and application-level access for security purposes, to the Apple File System (APFS), designed to support strong encryption, snapshotting, and modern storage management on mobile devices [19], [20]. On mobile platforms, user data is frequently stored within SQLite databases, Extensible Markup Language (XML), and JavaScript Object Notation (JSON) files. In contrast, application data is sandboxed in application-specific directories on both major platforms (e.g., /data/data/ on Android and per-application container directories on iOS), requiring forensic tools to understand app-specific paths and structures [16], [17], [18], [21], [22], [23]. This makes user-data partitions on mobile devices central targets for forensic extraction because they hold most user-generated content and application data, often at a granularity not typical in traditional desktop forensics [17].

Security architectures on modern mobile devices further complicate forensic acquisition. Modern mobile devices implement stringent protections, including File-Based Encryption (FBE) using 256-bit Advanced Encryption Standard (AES), metadata encryption, secure boot, and hardware-backed key management through Trusted Execution Environments (TEE). These protections, such as Android's

mandatory FBE in recent versions, are coupled with authentication safeguards like stretched credentials, tokens, and secure hashes, meaning physical possession of a device no longer guarantees access to its data. This widens the gap between device-level security and the capabilities of forensic tools [16].

Mobile devices are also characterised by high data volatility. Limited storage capacity, application behaviour, and automated system processes can rapidly overwrite or purge data [1], [24]. Moreover, the application-centric design of mobile platforms distributes user data across numerous apps—such as messaging, navigation, and browsers—each with distinct permission models, storage schemes, and artefact formats [16], [18]. Factory reset mechanisms on modern Android and iOS smartphones often invalidate encryption keys rather than directly wiping raw storage, rendering data unrecoverable even if it physically remains, unless cryptographic keys can be recovered [16].

Finally, mobile devices are tightly integrated with cloud services and external networks, creating external dependencies that extend investigations beyond the physical handset. Artefacts such as accounts, tokens, synchronisation metadata, and usage logs may remain on the device, but the underlying content is frequently stored in remote services and may be encrypted or accessible only through legal processes. These developments have shifted mobile forensics from a purely device-centric activity to a multi-platform endeavour that must consider both on-device artefacts and associated cloud environments [2], [25], [26], [27].

Taken together, platform diversity, file-system variation, stringent encryption, data volatility, app-centric storage, and cloud integration underscore the need for robust and well-structured forensic processes specifically tailored to mobile devices.

2.2 NIST SP 800-101 Rev. 1 mobile forensic process model

NIST SP 800-101 Rev. 1 defines a four-phase mobile device forensic process model: Preservation, Acquisition, Examination & Analysis, and Reporting [1]. This model has become widely adopted in both professional practice and academic research for mobile device investigations

The phases, as defined by Ayers et al. [1], are illustrated in Fig.1:

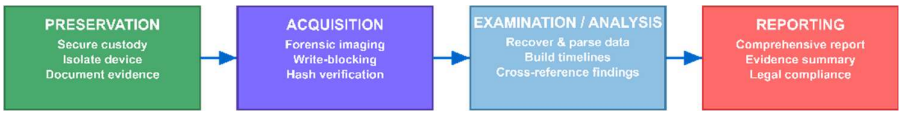

Fig. 1. Four Phases of the NIST Mobile Device Forensic Process [1].

- Preservation: This phase focuses on maintaining the integrity and original state of mobile devices and associated evidence from the moment they are identified or seized. Key activities include securing the scene, controlling the scene, isolating devices from networks (e.g., using Faraday bags or disabling radios), and documenting, packaging, transporting, and storing evidence in accordance with established procedures. The objective is to prevent alteration, loss, or destruction of data before forensic analysis.

- Acquisition: The acquisition phase involves creating a forensically sound copy or extraction of data from the target device and related media. Investigators establish connections between the device and acquisition systems and select appropriate acquisition techniques—manual, logical, physical, or chip-off—based on the device and investigative requirements. Documentation of tool versions, procedures, and device state is critical, and data integrity is preserved through mechanisms such as write blockers and cryptographic hash verification. The outcome is a reliable and authentic duplicate or extraction suitable for forensic examination.
- Examination/Analysis: This phase aims to uncover, interpret, and evaluate digital evidence from the acquired data. All examination and analysis activities are conducted on forensic copies of the acquired data rather than on the original evidence to preserve evidential integrity and maintain the chain of custody. Examiners use specialised tools to navigate, search, decode, and analyse visible and deleted data, correlate artefacts across applications and logs, and distinguish relevant from irrelevant information. Typical analyses include ownership attribution, application and file usage reconstruction, temporal sequencing, and identification of hidden or encrypted content, sometimes corroborated with external data sources such as provider records.
- Reporting: The reporting phase produces a comprehensive, accurate record of the forensic process and findings. This includes documenting each step from preservation through analysis, the methods and tools used, relevant case information, and supporting artefacts such as logs, screenshots, and examiner notes. The report must be understandable to non-technical stakeholders and support peer review, reproducibility, and legal scrutiny.

2.3 **ISO/IEC 27000-family standards and digital forensics**

The ISO/IEC 27000 family provides a complementary, domain-neutral set of standards that address key aspects of digital evidence handling and investigation across multiple phases of the forensic process [7], [8], [9], [10]. Rather than prescribing a single forensic workflow, the standards adopt a modular approach, allowing organisations to apply relevant guidance depending on investigative scope, technology, and legal context.

ISO/IEC 27043 defines general principles and phases of digital investigations, serving as a high-level investigative framework upon which other standards build (ISO/IEC, 2015b). ISO/IEC 27037 offers specific guidance on identification, collection, acquisition, and preservation of digital evidence, aligning closely with the preservation and acquisition phases of the NIST SP 800-101 forensic process [7]. ISO/IEC 27040 provides guidance on storage security and is relevant once digital evidence has been secured and retained [28]. ISO/IEC 27042 focuses on the analysis and interpretation of digital evidence, emphasising structured reasoning, documentation of methods, and transparency of analytical decisions, and is particularly relevant to the examination stages [10].

ISO/IEC 27041 provides a cross-cutting framework for validating forensic methods and tools, emphasising that techniques must be demonstrably reliable and fit for purpose across all phases of an investigation [8]. In parallel, the ISO/IEC 27050 series,

originating from electronic discovery, addresses organisational and legal aspects of digital evidence management, including chain of custody and legal defensibility [29].

These standards, primarily developed by ISO/IEC Joint Technical Committee 1/ Subcommittee 27 (JTC 1/SC 27), aim to ensure consistency in terminology, structure, and methodology across the family. They emphasise ongoing responsibilities—maintaining data integrity, documenting processes, and ensuring procedural transparency—that extend beyond any single investigation phase. Their modular and adaptable nature has led to increasing adoption in diverse digital forensic contexts, including mobile device investigations.

Given the focus of this study on mobile device forensics rather than organisational eDiscovery governance, selective adoption of the ISO/IEC 27050 series is required. While the ISO/IEC 27050 series as a whole addresses electronic discovery, only ISO/IEC 27050-1 and ISO/IEC 27050-3 align directly with the NIST SP 800-101 forensic process. Other parts of the series focus on organisational governance, jurisdictional compliance, or technical readiness and therefore fall outside the scope of phase-based forensic analysis [29], [30].

2.4 Fragmentation in mobile forensic process models

Although many frameworks describe the digital forensic process with different terminology, they generally retain similar high-level phases and a similar chronological order. For example, the EC-Council's Computer Hacking Forensic Investigator (CHFI) model adopts pre-investigation, investigation, and post-investigation phases. At the same time, the Association of Chief Police Officers (ACPO) Good Practice Guide and European Network of Forensic Science Institutes (ENFSI) frameworks use variations of plan/capture/analyse/present or identify/acquire/analyse/report [31], [32], [33]. Despite this surface-level consistency, substantial variation exists beneath the terminology.

Al-Dhaqm et al. [34] conducted a comprehensive review of 100 mobile forensic investigation process models (MFIPMs) spanning two decades, uncovering the true extent of methodological diversity in the field. Their study revealed widespread inconsistencies, including ambiguous terminology, redundant phases, and limited applicability across different mobile platforms. These findings suggest that, although high-level frameworks may appear similar, their practical implementation varies significantly.

In response to these inconsistencies, Al-Dhaqm et al. [34] proposed the Harmonised Mobile Forensic Investigation Process Model (HMFIPM), which consolidates typical phases —preparation, acquisition, preservation, examination, analysis, reporting, and presentation — into a unified structure intended to standardise investigative workflows. This harmonisation effort aims to bridge the gap between theoretical consistency and practical fragmentation.

Similarly, Ali et al. [35] proposed a conceptual metamodel for mobile forensics after analysing thirteen existing process models. They identified four foundational phases: Preservation, Acquisition, Examination, and Analysis, which align with those in NIST SP 800-101 Rev. 1. These core phases are supported by additional conceptual elements, including activities, entities, and actors. Rather than prescribing a fixed sequence of

steps, the metamodel provides a domain-level abstraction that facilitates the reuse and harmonisation of concepts across different mobile forensic tools and models.

More recent efforts continue to grapple with these standardisation challenges. Moreb et al. [36] developed the Mobile Forensics Investigation Process Framework (MFIPF), which organises investigations into four phases: Data Preparation, Information Analysis, Case Construction, and Case Closing. Their work demonstrates the ongoing nature of fragmentation issues identified by earlier researchers, as they found significant variations in forensic tool effectiveness, with accuracy rates ranging from 9.84% to 78.69% depending on the approach used. The MFIPF framework attempts to address these inconsistencies by providing detailed, mobile-specific procedures for each investigation phase. However, like previous harmonisation efforts, the framework remains primarily theoretical and lacks empirical validation, underscoring the persistent challenge of translating comprehensive procedural models into demonstrably effective practice.

Compared with these models, the proposed framework does not introduce another standalone mobile forensic process model. Instead, it uses NIST SP 800-101 Rev. 1 as the operational backbone and maps ISO/IEC 27000-family standards onto each phase to connect mobile forensic activities with governance, documentation, analysis, and validation requirements. HMFIPM primarily addresses process harmonisation, Ali et al.'s metamodel provides a domain-level abstraction, and MFIPF offers detailed mobile investigation procedures; however, these models do not explicitly integrate NIST's mobile forensic phases with ISO/IEC validation and defensibility requirements. The proposed framework, therefore, contributes a standards-aligned reference model that connects operational activities, mobile-specific constraints, evidential documentation, and cross-phase validation.

The rapid evolution of mobile technologies further exacerbates the problem. Devices and operating systems evolve faster than tools and methodologies can adapt, particularly where strong security features, proprietary file systems, and cloud-integrated services are involved [14]. Models effective for earlier device generations may not apply to modern smartphones that implement advanced encryption, decentralised storage, and frequent updates. Methodological priorities also differ across frameworks—some emphasise acquisition and data extraction, while others focus on post-acquisition analysis and interpretation—leading to divergent and often incompatible approaches [37], [38].

In summary, while the NIST model and ISO/IEC standards provide widely recognised guidance, there is no single, widely adopted, integrated process framework that systematically combines them in a way that is explicitly tailored to the practical constraints of contemporary mobile devices. This motivates the integrated conceptual NIST–ISO/IEC framework presented in the next section.

3 Integrated Conceptual NIST–ISO/IEC Framework for Mobile Device Forensics

Building on the challenges and fragmentation identified in the preceding sections, this section proposes an integrated conceptual framework for mobile device forensics that aligns established operational guidance with international governance and validation

standards. Rather than introducing a new investigative process, the framework synthesises the phase-based structure of NIST SP 800-101 Rev. 1 with complementary ISO/IEC standards to clarify how operational activities, evidential handling requirements, and validation expectations interact across the mobile forensic lifecycle. The objective is to provide a coherent, standards-aligned conceptual framework that supports consistent decision-making, documentation, and defensibility in mobile investigations, while remaining adaptable to evolving device architectures, platforms, and security mechanisms.

3.1 Design principles

The proposed conceptual framework is guided by three main design principles:

1. Operational backbone: NIST SP 800-101 Rev. 1 provides the core four-phase workflow—Preservation, Acquisition, Examination & Analysis, and Reporting—that structures the sequence of activities in mobile investigations.
2. Governance and validation: ISO/IEC standards are mapped onto each NIST phase to supply high-level governance, assurance, and validation requirements, with ISO/IEC 27041 explicitly treated as a cross-cutting validation layer spanning the entire process.
3. Mobile specificity: Contemporary mobile-specific challenges—platform diversity, file-system variation, application sandboxing, encryption, volatility, and cloud integration—are explicitly incorporated into the tasks, controls, and artefact handling strategies at each phase.

This integration aims to reduce methodological fragmentation by providing clear, standards-aligned guidance while remaining adaptable to new device families and operating system versions.

Taken together, these design principles motivate the development of an integrated conceptual framework that brings together operational guidance from NIST SP 800-101 Rev. 1 with complementary ISO/IEC standards. To clarify the relationships between investigation phases, phase-specific standards, and cross-cutting governance and validation layers, the proposed framework is summarised visually in Fig. 2

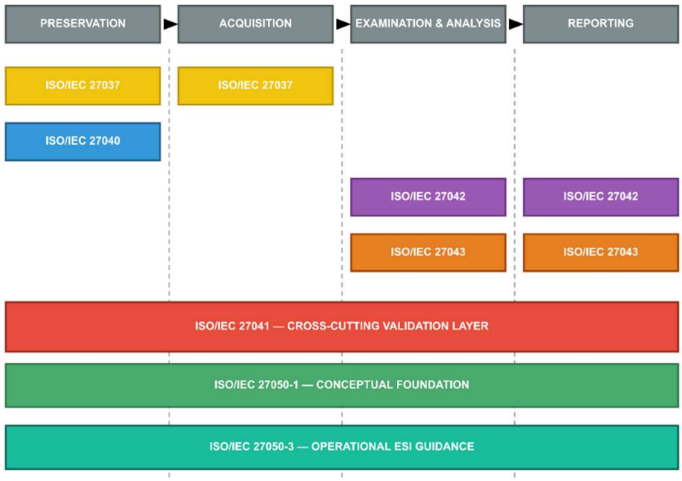

Fig. 2. Integrated conceptual NIST–ISO/IEC framework for mobile device forensics

Fig. 2 serves as a reference model for the discussion that follows. It shows how the NIST SP 800-101 phases provide the operational structure of the framework, while ISO/IEC standards contribute governance, documentation, analysis, and validation requirements across the mobile forensic lifecycle. Sections 3.2 and 3.3 elaborate on these relationships in detail, explaining how each NIST phase is supported by relevant ISO/IEC standards and how validation is treated as a continuous, cross-phase activity.

3.2 Phase-by-phase integration

Having established the framework's design principles and overall structure, this section applies it in a phase-by-phase manner. The NIST SP 800-101 Rev. 1 phases are used as the primary structural backbone. Relevant ISO/IEC standards are mapped to each phase to clarify how governance, documentation, and validation support operational forensic activities.

While ISO/IEC 27050-3 provides operational guidance for electronic discovery activities, it is conceptually grounded in ISO/IEC 27050-1, which establishes the definitions, scope, and structure of the electronic discovery process. Accordingly, the phase-by-phase integration presented here is interpreted within the conceptual framework defined by ISO/IEC 27050-1, with phase-specific guidance drawn from ISO/IEC 27050-3, NIST SP 800-101, and related ISO/IEC standards.

This approach clarifies how different standards contribute at each stage of a mobile forensic investigation, while preserving the logical progression of activities from initial preservation through acquisition, examination/ analysis, and reporting, as summarised in Fig. 2.

Preservation. NIST's Preservation phase is primarily concerned with maintaining the original condition of digital evidence from identification or seizure onwards. In this framework, preservation is understood at two complementary levels: forensic device preservation, which focuses on protecting the physical and logical state of digital devices at the point of seizure, and Electronically Stored Information (ESI) preservation, which focuses on maintaining the integrity, provenance, and traceability of ESI.

ISO/IEC 27037 reinforces forensic device preservation by providing detailed guidance on identifying, collecting, acquiring, and preserving digital evidence, while ISO/IEC 27040 can be referenced for storage and security considerations once evidence has been secured.

Mobile-specific preservation activities involve evaluating and controlling the incident scene to minimise risks such as remote wiping, remote locking, or data alteration via network connectivity. Devices may be isolated from wireless networks through Faraday bags, airplane mode, or disabling radios, while taking care not to alter volatile data unnecessarily. Preservation activities must also consider device power state in relation to on-device encryption schemes, for instance deciding whether to maintain a powered-on but locked device to preserve decrypted memory contexts, or to power off the device to prevent further remote interference. Device characteristics (model, OS version, visible security features), visible status (locked/unlocked, powered on/off), and environmental conditions should also be documented in accordance with ISO/IEC 27037's emphasis on proper documentation.

ISO/IEC 27041's validation perspective contributes by requiring that preservation methods and tools (e.g., Faraday equipment and logging procedures) be demonstrated to be reliable and repeatable. In parallel, ISO/IEC 27050-1 and ISO/IEC 27050-3 support preservation at the ESI level, with ISO/IEC 27050-1 defining the foundational concepts of chain of custody and provenance, and ISO/IEC 27050-3 providing requirements and guidance for ESI preservation that emphasise documentation, transparency, and defensibility. Together, these standards support continuous documentation of ESI handling, while avoiding prescriptive technical requirements at the device level.

Acquisition. NIST SP 800-101 defines the Acquisition phase as the creation of a forensically sound copy or extraction of data from mobile devices. ISO/IEC 27037 again provides guidance on acquisition methods and associated documentation requirements, while ISO/IEC 27050-3 contributes principles from electronic discovery that inform collection, accuracy, and documentation in legally defensible contexts.

For mobile devices, the framework recommends selecting acquisition techniques (manual, logical, file system, physical, chip-off, or micro-read) based on the device state, platform, security features, and investigative scope. Strong encryption, secure boot mechanisms, and hardware-backed key storage may limit the feasibility of physical or chip-off acquisition. In many contemporary devices, acquiring logical or file system information via standard interfaces may be the only practical and proportionate approach. The framework also recommends documenting the acquisition environment, including tool names and versions, connection methods, device state (e.g., unlocked with consent, locked, or temporarily bypassed), and any bypass or access-enabling techniques employed. Cryptographic hash values of acquired images or

extracted datasets should also be generated and recorded to support later integrity verification, while acknowledging that hashing alone may not detect sophisticated anti-forensic activity or pre-existing compromise.

ISO/IEC 27041 further strengthens this phase by introducing a validation and assurance perspective, requiring that acquisition tools and methods be tested and verified—ideally against reference datasets—before deployment in operational cases. It also emphasises that limitations arising from platform security controls, proprietary interfaces, or restricted access mechanisms should be explicitly acknowledged.

The framework, therefore, encourages practitioners to treat acquisition not merely as a technical extraction step, but as a documented and justifiable decision process, grounded primarily in NIST SP 800-101 and supported by ISO/IEC 27037, ISO/IEC 27041, and ISO/IEC 27050-3 requirements for evidential reliability, transparency, and defensibility.

Examination/Analysis. The NIST Examination/Analysis phase transforms acquired data into actionable forensic insight, encompassing navigation, decoding, searching, correlation, and interpretation of artefacts. Within the ISO framework, ISO/IEC 27050-3 distinguishes between ESI processing (preparation and structuring of data) and ESI analysis (interpretation and reasoning), while ISO/IEC 27042 and ISO/IEC 27043 provide guidance on analysis techniques, interpretation, and investigative structuring.

Applied to mobile devices, the integrated conceptual framework structures examination and analysis activities around four primary artefact domains, reflecting NIST guidance and ISO/IEC 27050-3's distinction between processing and analysis:

- System-level data: System logs, boot records, crash reports, and update histories can reveal device state, operating conditions, evidence of tampering, and temporal anchors for events.
- User-generated content: Call logs, SMS/MMS messages, contacts, photographs, videos, and documents provide direct evidence of user communications and activities.
- Application-specific artefacts: Application databases (commonly SQLite), XML or JSON preference files, log files, and protocol buffer data stored within application-specific directories yield fine-grained insight into user behaviour within individual applications.
- Contextual metadata: Timestamps, geolocation data, network identifiers (e.g., Service Set Identifiers (SSIDs), Internet Protocol (IP) addresses), permissions, and file paths form the contextual backbone for reconstructing timelines, locations, and relationships between artefacts.

Within this structure, the conceptual framework encourages examiners to leverage contemporary artefacts, including device logs, system statistics, user behaviour records, and application usage metadata, to construct high-level representations of device state. Metadata (e.g., timestamps, file paths, application attributes, and system logs) should be systematically extracted, normalised, and organised to support timeline reconstruction and evidential authentication. The framework also encourages consistency and correlation checks across artefacts and metadata, such as aligning application-level logs with system events and network

records, to identify partial extractions, inconsistencies, user manipulation, or potential anti-forensic activity.

ISO/IEC 27042 and ISO/IEC 27043 support these activities by emphasising structured analysis, the correlation of evidence, the documentation of analytical reasoning, and the clear articulation of investigative hypotheses and conclusions. ISO/IEC 27041's validation perspective reinforces the need for repeatability and reliability during examination and analysis, encouraging cross-tool comparison and confirmation—for example, verifying that multiple forensic tools yield consistent interpretations of key mobile artefacts.

Reporting. NIST SP 800-101 defines the Reporting phase as the formal documentation and communication of forensic findings, methods, and limitations. Within the ISO framework, ISO/IEC 27042 and ISO/IEC 27043 provide complementary guidance on documentation, interpretation, investigative conclusions, and legal defensibility, while ISO/IEC 27050-3 contributes requirements for transparency, documentation, and formal production of results in contexts where evidence may be subject to legal scrutiny.

In mobile-focused investigations, the integrated framework recommends that reports clearly document the end-to-end forensic process, including preservation actions, acquisition methods, examination and analysis steps, and the rationale for methodological choices made in light of device security features and platform constraints. Reports should also explain mobile-specific challenges—such as full-disk encryption, application sandboxing, cloud-resident data, and data volatility—to non-technical stakeholders, clarifying why certain artefacts may be unavailable, or only partially recoverable. Reports should further present structured summaries of key artefact categories, timelines, and correlations, demonstrating how system-level data, user-generated content, and application-specific artefacts were combined to support investigative findings. Sufficient technical detail, including tool names and versions, cryptographic hash values, configuration settings, and processing parameters, should be preserved to enable peer review, repeatability, and independent re-analysis, in accordance with ISO/IEC expectations for transparency and reproducibility.

ISO/IEC 27050-3's emphasis on defensible production and documentation is reflected in meticulous tracking of evidence handling, access, and transformation throughout the investigation. This ensures that both physical devices and derived forensic artefacts can be accounted for in an auditable manner, supporting evidential reliability and admissibility when findings are presented to courts, regulators, or other external stakeholders.

3.3 Cross-cutting validation layer

A defining feature of the integrated framework is the explicit treatment of validation as a continuous, cross-phase activity rather than a one-off step. ISO/IEC 27041 underpins this approach by requiring that tools, methods, and procedures be demonstrably reliable for their intended use.

Drawing on existing validation research, the framework advocates a layered post-acquisition validation model for mobile device data, including:

- Integrity verification: Applying hashing algorithms such as Message-Digest Algorithm 5 (MD5) or Secure Hash Algorithm 256-bit (SHA-256) to acquired images or extractions at multiple stages to detect accidental modifications, while recognising that advanced anti-forensic actions can circumvent simple hash-based checks.
- Consistency checks: Cross-referencing artefacts, metadata, and timestamps across system logs, app records, and user content to identify discrepancies that might indicate incomplete extraction or tampering.
- Source reliability: Prioritising data from trusted system directories and verified application paths, thereby reducing the risk of analysing injected or spoofed artefacts.
- Schema and format validation: Ensuring that database structures and log formats conform to expected schemas, which can reveal corruption, deliberate manipulation, or analytical errors.

These validation steps are positioned between Acquisition and Examination/Analysis but conceptually span the entire process, reinforcing evidentiary credibility before deep analysis begins.

4 Implications for tool selection and validation

This section applies the integrated conceptual framework to a representative mobile device investigation, illustrating how NIST phases and ISO/IEC principles inform investigative decision-making, documentation, and validation activities. The illustrative scenario is intended to demonstrate practical application of the framework rather than prescribe a fixed investigative procedure.

4.1 Illustrative application of the integrated framework

To illustrate the practical use of the integrated framework, consider a hypothetical investigation involving a seized smartphone running a modern mobile operating system with robust encryption and secure boot enabled.

Preservation. Investigators secure the physical scene, isolate the device from networks using a Faraday enclosure or equivalent techniques, and document its status and visible characteristics (e.g., model, OS version, and presence of biometric locks). Decisions about powering down or maintaining the current state are made with reference to the implications for on-device encryption and potential volatile artefacts.

Acquisition. Based on the device state and legal authority, investigators select an acquisition strategy—e.g., logical extraction via a supported forensic tool or interface—while documenting tool versions and connection methods. Cryptographic hashes of the acquired data are calculated and recorded, while limitations arising from encryption and restricted low-level access are explicitly documented. Prior to complete analysis, hashes are reverified and consistency checks are performed, for instance verifying that

log timestamps align with device time settings and that key databases are structurally intact. Any anomalies indicating partial extractions or manipulation are documented, and additional acquisitions or cross-tool comparisons are considered where necessary.

Examination/Analysis. Examiners parse system logs, user communications, app databases, and metadata using a combination of commercial suites and specialised open-source tools. They reconstruct user activity timelines, correlate app events with system logs and network connections, and identify relevant communications or locations.

Reporting. Finally, a structured report is produced that explains the methodology, device-specific constraints, artefacts examined, timelines reconstructed, and the confidence level associated with key findings. The report explicitly ties evidence handling and analysis to NIST phases and ISO/IEC principles, aiding legal scrutiny and peer review.

4.2 Proposed evaluation criteria

Although the illustrative application demonstrates how the framework can guide mobile forensic decision-making, empirical validation would require measurable evaluation criteria. Future assessments of the framework could, therefore, consider metrics such as evidence completeness, cross-tool consistency, reproducibility of acquisition and analysis results, error and discrepancy rates, and documentation quality.

Evidence completeness may be assessed by comparing recovered artefacts against known datasets or expected case profiles, while cross-tool consistency may evaluate whether different forensic tools produce comparable artefact interpretations, timestamps, metadata, and application records. Reproducibility may assess whether independent examiners following the framework generate consistent acquisition logs, timelines, analytical findings, and reporting outputs. Additional measures, including parsing errors, incomplete extractions, timestamp conflicts, hash verification failures, and documentation completeness, may further support evaluation of evidential reliability and defensibility.

These criteria provide a basis for future experimental validation of the framework using controlled datasets, comparative tool analysis, and real-world mobile forensic scenarios.

4.3 Implications for tool selection and validation

The conceptual framework does not prescribe specific tools but provides a standards-aligned rationale for adopting a hybrid toolchain that combines commercial and open-source solutions. Commercial tools are widely used in professional environments due to their integrated acquisition, analysis, and reporting features and because they generally provide vendor support and regular updates. However, they can be costly and may lack flexibility for specialised tasks or emerging artefacts [1], [39], [40].

Open-source tools, by contrast, provide customisability and are often extended by practitioners to handle niche or novel artefacts that commercial tools may not fully support. They may, however, suffer from limited formal support and incomplete documentation, which can present challenges in legal contexts [40], [41]. Within the integrated framework, ISO/IEC 27041 and 27042 encourage cross-tool validation: findings from one tool should, where possible, be corroborated by another, and discrepancies must be investigated and documented. This aligns with best-practice recommendations that advocate using multiple tools within the same investigation to maximise coverage and reduce reliance on any single solution.

5 Discussion

The integrated NIST–ISO/IEC framework for mobile device forensics offers several advantages. It aligns a well-established mobile-specific process model (NIST SP 800-101) with internationally recognised standards for digital investigations, evidence handling, and tool validation, thereby strengthening procedural rigour and legal defensibility. It explicitly integrates mobile-specific challenges into each phase, reducing the risk that generic process models overlook critical constraints such as strong encryption, application sandboxing, or cloud dependencies.

The framework also addresses a key source of fragmentation identified in the literature: the proliferation of divergent mobile forensic process models and the lack of unified, standards-aligned, and platform-aware approaches. By providing a clear mapping between NIST phases, ISO/IEC standards, and mobile artefact domains, it can serve as a reference for practitioners designing standard operating procedures and for researchers developing or evaluating forensic tools and methods.

However, the framework has limitations. It is primarily conceptual and has not yet been empirically evaluated across a broad range of real-world mobile cases or devices. It also relies on ISO/IEC standards that, by design, are high-level and technology-neutral, leaving room for interpretive differences in implementation. Moreover, the rapid evolution of mobile platforms—new security features, file systems, and application behaviours—means that the framework will require periodic revision to remain fully relevant.

Future work should include systematic case studies in which the framework is applied to controlled and real-world mobile investigations using the validation metrics proposed in Section 4.2. It could also inform the development of tool-agnostic checklists and templates for each phase, making it easier for organisations to operationalise the framework in practice.

6 Conclusion

Mobile devices present unique and evolving challenges to digital forensics, including platform fragmentation, advanced encryption, application-centric evidence, high data volatility, and deep cloud integration. While NIST SP 800-101 Rev. 1 and the ISO/IEC 27000-family standards each provide valuable guidance, they have often been applied

separately and without explicit tailoring to the practical context of modern mobile devices.

This paper proposes an integrated conceptual framework that uses NIST's four-phase model as the operational backbone and embeds ISO/IEC governance and validation principles throughout the lifecycle of mobile device investigations. By structuring artefact handling, acquisition decisions, analysis workflows, reporting practices, and validation activities within a unified standards-aligned model, the framework aims to reduce methodological fragmentation and enhance the defensibility and repeatability of mobile digital forensics. As mobile ecosystems continue to evolve, such integrated, standards-based frameworks will be essential to sustaining reliable forensic practice and enabling robust evaluation of tools and methodologies.

References

1. Ayers, R., Brothers, S., Jansen, W.: *Guidelines on Mobile Device Forensics*. NIST Special Publication 800-101 Rev. 1, National Institute of Standards and Technology, Gaithersburg, MD (2014).
2. Barmpatsalou, K., Cruz, T., Monteiro, E., Simoes, P.: Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys* 51(3) (2019).
3. Bernardo, B.M.V., Mamede, H.S., Barroso, J.M.P., Dos Santos, V.M.P.D.: Mobile device forensics framework: A toolbox to support and enhance this process. *Emerging Science Journal* 8(3), 972–998 (2024).
4. Almuqren, A., Alsuwaelim, H., Rahman, M.M.H., Ibrahim, A.A.: A systematic literature review on digital forensic investigation on Android devices. In: *Procedia Computer Science*. Elsevier, 1332–1352 (2024).
5. Fukami, A., Stoykova, R., Geradts, Z.: A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation* 38 (2021).
6. Patel, B., Mann, P.S.: A survey on mobile digital forensic: Taxonomy, tools, and challenges. *Security and Privacy* 8, e470 (2025).
7. ISO/IEC 27037:2012: *Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*. ISO, Geneva (2012).
8. ISO/IEC 27041:2015: *Information Technology — Security Techniques — Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods*. ISO, Geneva (2015).
9. ISO/IEC 27043:2015: *Information Technology — Security Techniques — Incident Investigation Principles and Processes*. ISO, Geneva (2015).
10. ISO/IEC 27042:2015: *Information Technology — Security Techniques — Guidelines for the Analysis and Interpretation of Digital Evidence*. ISO, Geneva (2015).
11. Aljahdali, A., Alsaidi, N., Alsafri, M., Alsulami, A., Almutairi, T.: Mobile device forensics. *Revista Romana de Informatica si Automatica* 31(3), 81–96 (2021).
12. Chen, S.W., Yang, C.H., Liu, C.T.: Design and implementation of live SD acquisition tool in Android smartphone. In: *Proc. 5th Int. Conf. on Genetic and Evolutionary Computing (ICGEC)*. IEEE, 157–162 (2011).
13. Junior, O.L., Keita, M.K., Fall, D., Diop, I.: Android digital forensics: State of the art. In: *Proc. IEEE Conference*. IEEE, 1–7 (2025).
14. Fakiha, B.: Unlocking digital evidence: Recent challenges and strategies in mobile device forensic analysis. *Journal of Internet Services and Information Security* 14(2), 68–84 (2024).
15. Kaur, H., Choudhary, K.R.: Digital forensics: Implementation and analysis for Google Android framework. In: *Studies in Computational Intelligence*, vol. 691. Springer, 307–331 (2017).

16. Blankesteijn, M.B., Fukami, A., Geradts, Z.J.M.H.: Assessing data remnants in modern smartphones after factory reset. *Forensic Science International: Digital Investigation* 46 (2023).
17. Hazra, S., Mateti, P.: Challenges in Android forensics. In: *Communications in Computer and Information Science*. Springer, 286–299 (2017).
18. Pieterse, H.: Mobile forensics: Beyond traditional sources of digital evidence. In: *Proc. European Conf. on Information Warfare and Security (ECCWS)*. Curran Associates, 295–303 (2020).
19. Nordvik, R.: APFS. In: *Mobile Forensics – The File Format Handbook*. Springer, 3–39 (2022).
20. Göbel, T., Türr, J., Baier, H.: Revisiting data hiding techniques for Apple File System. In: *ACM International Conference Proceeding Series*. ACM (2019).
21. Park, J., Park, J., Kim, H., Kang, S., Kim, J.: A comprehensive artifact analysis of Google applications on Android and iOS platforms. *Forensic Science International: Digital Investigation* 55 (2025).
22. Rao, V.V., Chakravarthy, A.S.N.: Forensic analysis of Android mobile devices. In: *Proc. Int. Conf. on Recent Advances and Innovations in Engineering (ICRAIE)*. IEEE (2016).
23. Vidas, T., Zhang, C., Christin, N.: Toward a general collection methodology for Android devices. In: *Proc. DFRWS Annual Conference*. Digital Forensic Research Workshop (2011).
24. Wachter, P., Gruhn, M.: Practicability study of Android volatile memory forensic research. In: *Proc. IEEE Int. Workshop on Information Forensics and Security*. IEEE (2015).
25. Montasari, R., Hill, R.: Next-generation digital forensics: Challenges and future paradigms. In: *Proc. IEEE Int. Conf. on Global Security, Safety and Sustainability (ICGS3)*. IEEE, 205–212 (2019).
26. Jones, A., Vidalis, S.: Rethinking digital forensics. International Association for Educators and Researchers (IAER) (2019).
27. Singano, T. et al.: Digital forensics investigations: Major challenges in mobile and cloud forensics. In: *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (LNICST)*. Springer, 35–53 (2025).
28. ISO/IEC 27040:2024: *Information Technology — Security Techniques — Storage Security*. ISO, Geneva (2024).
29. ISO/IEC 27050-1:2016: *Information Technology — Security Techniques — Electronic Discovery — Part 1: Overview and Concepts*. ISO, Geneva (2016).
30. ISO/IEC 27050-3:2017: *Information Technology — Security Techniques — Electronic Discovery — Part 3: Code of Practice for Electronic Discovery*. ISO, Geneva (2017).
31. Association of Chief Police Officers (ACPO): *ACPO Good Practice Guide for Digital Evidence*, Version 5 (2011).
32. EC-Council: *Computer Hacking Forensic Investigator (CHFI) Course Outline*, Version 10 (2021).
33. European Network of Forensic Science Institutes (ENFSI): *Best Practice Manual for the Forensic Examination of Digital Technology*, Version 1 (2015).
34. Al-Dhaqm, A., Razak, S.A., Ikuesan, R.A., Kebande, V.R., Siddique, K.: A review of mobile forensic investigation process models. IEEE (2020).
35. Ali, A., Razak, S.A., Othman, S.H., Mohammed, A., Saeed, F.: A metamodel for mobile forensics investigation domain. *PLoS ONE* 12(4) (2017).
36. Moreb, M., Salah, S., Amro, B.: A novel framework for mobile forensics investigation process. *International Journal of Computing and Digital Systems* 16(1), 125–136 (2024).
37. Ahmed, R., Dharaskar, R.V., Thakare, V.M.: Efficient generalized forensics framework for extraction and documentation of evidence from mobile devices. *International Journal of Enhanced Research in Management and Computer Applications* 2 (2013).
38. Alzaabi, M.: Ontology-based forensic analysis of mobile. In: *Proc. IEEE Int. Conf. on Electronics, Circuits, and Systems (ICECS)*. IEEE, 64–65 (2013).

39. Delija, D., Sudec, D., Sirovatka, G., Zagar, M.: How to do a forensic analysis of Android 11 artifacts. In: *Proc. MIPRO Jubilee Int. Convention on Information, Communication and Electronic Technology*. IEEE, 1042–1047 (2022).
40. Hargreaves, C., Breitinger, F., Dowthwaite, L., Webb, H., Scanlon, M.: DFPulse: The 2024 digital forensic practitioner survey. *Forensic Science International: Digital Investigation* 51 (2024).
41. Cohen, F.: *Digital Forensic Evidence Examination*. 5th edn. Fred Cohen & Associates, Livermore, CA (2013).