

Original Article

Digital Forensics and Evidentiary Admissibility in Cross-Border Cybercrime Investigations: A Comparative Analysis of UK, EU, and Emerging Jurisdictions

Rashid Hussain

Nour Internet Company for communication & IT, Riyadh, Saudi Arabia.

Student of University of East London for MSc Information Security and Digital Science.

Received: 09-03-2026

Revised: 09-24-2026

Accepted: 09-29-2026

Published: 10-03-2026

ABSTRACT

The transnational nature of cybercrime has created significant challenges for the lawful acquisition, preservation, authentication and admissibility of digital evidence across national borders. These challenges are intensified by cloud computing, distributed data storage, service-provider control, encryption, differing procedural safeguards and variations in national evidentiary requirements. This study comparatively examines digital forensics and evidentiary admissibility in the United Kingdom, European Union, Saudi Arabia, India and South Africa. Using a qualitative comparative doctrinal legal methodology, it analyses legislation, international instruments, official materials and relevant scholarly literature concerning forensic acquisition, preservation, hashing, metadata, logs, timestamps, tool reliability, chain of custody, cross-border access, service-provider cooperation, privacy and judicial oversight. The analysis demonstrates substantial convergence around the importance of authenticity, integrity, reliability and preservation, but continuing divergence in the legal mechanisms governing acquisition, authentication and courtroom use. Particular challenges arise where cloud-based evidence is produced by service providers rather than directly acquired by forensic examiners, increasing the importance of provenance, metadata preservation and documented handling. The study finds that lawful acquisition and evidentiary admissibility are distinct but interconnected stages. Evidence may be obtained through a valid domestic or international mechanism yet remain vulnerable if its authenticity, integrity, provenance or chain of custody cannot subsequently be demonstrated. Effective cross-border digital-evidence cooperation therefore requires stronger interoperability between legal authority, digital-forensic standards, provider practices, data-protection safeguards and evidentiary requirements.

KEYWORDS

Digital Forensics, Digital Evidence, Cybercrime, Evidentiary Admissibility, Cross-Border Investigations, Cloud Evidence, Chain Of Custody, International Cooperation.

1. INTRODUCTION

1.1. Background to Cross-Border Cybercrime

Cybercrime increasingly operates across national boundaries, with offenders, victims, infrastructure, service providers and relevant evidence often located in different jurisdictions. Digital evidence may be stored across cloud platforms, communication services and data centres governed by different legal regimes. Investigators may therefore require cooperation from foreign authorities or private providers before evidence can be lawfully obtained.

Cross-border investigations involve both legal and technical challenges. Investigators must preserve relevant evidence while determining jurisdiction and the appropriate legal mechanism for acquisition. Mutual legal assistance remains important but may involve delays and procedural complexity. International frameworks have sought to address these difficulties. The Budapest Convention on Cybercrime supports cooperation on cybercrime and electronic evidence, while its Second Additional Protocol expands mechanisms for obtaining electronic evidence and cooperating with service providers. The European Union's e-Evidence framework, including Regulation (EU) 2023/1543, introduces European Production and Preservation Orders and applies from 18 August 2026.

1.2. Growth and Nature of Digital Evidence

Digital evidence is central to modern criminal investigations because communications, transactions, identities, locations and system activity are frequently recorded electronically. Its evidentiary value, however, depends on whether its origin, integrity, reliability and history can be demonstrated.

Digital data may be altered, deleted, encrypted, duplicated or transferred between systems and jurisdictions. Preservation and documentation are therefore essential. Casino et al. (2022) identify legal, procedural, technical and jurisdictional barriers as recurring problems in cross-border investigations. A defensible link must consequently be maintained between the original source, acquisition process, forensic examination and evidence presented in court.

1.3. Digital Forensics and the Evidentiary Process

Digital forensics involves the identification, preservation, acquisition, examination, analysis and documentation of electronic data. Evidentiary rules determine whether that material can be accepted and relied upon in court.

These processes are connected but distinct. Technically accurate acquisition does not automatically establish admissibility, while lawful access does not remove the need to demonstrate authenticity, integrity, reliability and continuity of custody. This issue is particularly significant where evidence is obtained under one jurisdiction's procedures but presented before a court applying another jurisdiction's evidentiary standards.

1.4. Problem Statement

The central problem is the potential gap between lawful cross-border acquisition and subsequent admissibility. Electronic evidence may be obtained through valid cooperation mechanisms yet remain vulnerable because of differences in procedural rules, authentication standards, privacy requirements and forensic practices.

James and Gladyshev (2016) identified communication, information-sharing and procedural weaknesses in mutual legal assistance involving digital evidence. These problems become more serious where evidence is volatile, remotely stored or controlled by private providers. The challenge is therefore not merely obtaining evidence, but obtaining it lawfully, reliably and transparently in a form capable of satisfying courtroom requirements.

1.5. Research Gap

Existing research examines cross-border electronic evidence, international cooperation, jurisdiction and digital-forensic practice, but these areas are often treated separately. Legal studies commonly focus on authority to obtain data, while forensic studies emphasise technical reliability. This study addresses this gap by integrating legal acquisition with preservation, forensic imaging, cryptographic hashing, metadata, logs, timestamps, tool validation, chain of custody and admissibility across the United Kingdom, European Union, Saudi Arabia, India and South Africa. Particular attention is given to cloud and provider-held evidence.

1.6. Research Questions

- What legal and forensic requirements govern the acquisition, preservation, authentication and admissibility of cross-border digital evidence?
- How do the UK, EU, Saudi Arabia, India and South Africa approach digital-evidence acquisition and admissibility?
- How do imaging, hashing, metadata, logs, timestamps, tool validation and chain of custody affect evidentiary reliability?
- What challenges arise from cloud, remotely stored and provider-controlled evidence?
- How can cooperation mechanisms preserve lawful acquisition while maintaining evidentiary reliability?

1.7. Research Objectives

The study aims to examine the relationship between lawful cross-border acquisition, forensic integrity and courtroom admissibility. It compares the five jurisdictions, evaluates key forensic safeguards, analyses cloud and provider-held evidence, and identifies measures for improving international cooperation without compromising procedural or evidentiary standards.

1.8. Significance and Contribution

The study's main contribution is its treatment of lawful acquisition, forensic integrity and admissibility as connected but distinct stages. Evidence may be lawfully obtained yet challenged where

provenance, integrity, chain of custody or forensic methodology cannot be adequately demonstrated. The comparative analysis also shows how different legal systems respond to shared technological challenges.

1.9. Scope and Delimitation

The study focuses on cross-border digital evidence involving the UK, EU, Saudi Arabia, India and South Africa. It examines acquisition, preservation, imaging, hashing, metadata, encryption, tool validation, authentication, chain of custody, cloud evidence, provider cooperation and admissibility. It does not examine every cybercrime offence or evidentiary rule.

1.10. Structure of the Article

The article first establishes the conceptual and forensic framework and methodology. It then examines international cooperation mechanisms and the legal frameworks of the selected jurisdictions. Subsequent sections compare evidentiary requirements, forensic integrity and cloud-forensics challenges before addressing policy implications, limitations, future research and conclusions.

2. CONCEPTUAL AND THEORETICAL FRAMEWORK

2.1. Concept of Digital Evidence

Digital evidence refers to information of potential evidentiary value that is created, stored, processed or transmitted electronically. It includes emails, messages, documents, images, videos, transaction records, metadata, logs, browser histories, location data, cloud records and information held by communication or online service providers.

Unlike physical evidence, digital data can be copied, modified, encrypted, deleted, remotely accessed or replicated across multiple systems and jurisdictions. Its evidentiary value therefore depends not only on content but also on provenance, acquisition method, integrity, preservation and documented handling. In this study, digital evidence means electronically generated or stored information capable of supporting or challenging a factual proposition in criminal proceedings when an adequate legal and forensic foundation is established.

2.2. Digital Forensics in Cybercrime Investigations

Digital forensics involves the identification, preservation, acquisition, examination, analysis and documentation of digital information for investigative and evidentiary purposes. Acquisition may involve forensic imaging, logical or physical collection, network capture, cloud extraction or provider-supplied records.

Where appropriate, forensic imaging enables examination without unnecessary alteration of the original source. Cryptographic hashing can help verify whether acquired data remain unchanged, but it should be supported by secure storage, documentation and chain-of-custody procedures. Forensic reliability also depends on documented tools and procedures, including software versions,

acquisition settings, errors and limitations. Tools and methods should, where appropriate, be validated or demonstrated to be fit for purpose to support reproducibility and independent evaluation.

2.3. Evidentiary Admissibility

Admissibility concerns whether evidence may legally be received by a court, while evidentiary weight concerns how much significance the court gives it. Digital evidence may require proof of relevance, authenticity, reliability, lawful acquisition and procedural compliance.

The central principle is:

Lawful acquisition $\neq$ automatic admissibility.

Evidence obtained through mutual legal assistance, production orders, preservation mechanisms or provider disclosure may still face challenge if authenticity, integrity, reliability or chain of custody cannot be adequately demonstrated.

2.4. Authentication, Integrity and Reliability

Authentication establishes that evidence is what it claims to be. Relevant indicators may include metadata, source information, account identifiers, provider records, witness testimony and hash values. Integrity concerns whether evidence has remained materially unchanged. Hashing can demonstrate consistency between acquired data and forensic copies, but it does not independently prove lawful acquisition or provenance.

Metadata, system logs and timestamps may provide important contextual evidence, although differences in time zones, clocks and provider systems can complicate timeline reconstruction. Reliability also depends on the source system, acquisition method, analytical technique, forensic tools and examiner interpretation.

2.5. Chain of Custody

Chain of custody records the history of evidence from identification and acquisition through examination, storage, transfer and courtroom presentation. Documentation should identify the source, acquisition date, examiner, method, hash values, forensic tools, transfers, storage conditions and significant analytical actions. Cross-border cases increase risk because evidence may pass through providers, foreign authorities, forensic laboratories, investigators, prosecutors and courts. Gaps may affect admissibility, evidentiary weight or credibility depending on the applicable jurisdiction.

2.6. Cloud and Cross-Border Electronic Evidence

Cloud evidence may involve users, investigators, service providers and infrastructure located in different jurisdictions. Relevant material may include communications, stored files, access logs, authentication records, IP data, backups and metadata.

Unlike traditional device examination, investigators may depend on provider exports, APIs or remote collection. Challenges include distributed storage, limited visibility into provider systems, short log-retention periods, changing metadata and encryption. Investigators should therefore document what was requested, what was supplied, how it was exported, what metadata accompanied it and how integrity was maintained. A lawful production order establishes authority to obtain data but does not automatically prove the authenticity or integrity of every item produced.

2.7. Jurisdiction and Remote Access

Digital infrastructure complicates territorial jurisdiction because data location may be uncertain, distributed or temporary. Technical ability to access remote data should not be confused with legal authority to acquire it. Cross-border investigations must distinguish technical capability, provider control, data location, investigative jurisdiction and lawful authority while preserving provenance and integrity after transfer.

2.8. Integrated Comparative Framework

The analysis adopts three interconnected stages:

Lawful Acquisition → Forensic Integrity → Courtroom Admissibility

Lawful acquisition covers jurisdiction, authority, preservation, international production and provider cooperation. Forensic integrity includes acquisition methods, hashing, metadata, logs, timestamps, encryption, tool validation, documentation and chain of custody. Courtroom admissibility considers authentication, reliability, provenance, procedural compliance and evidentiary weight. These stages remain distinct: lawful acquisition establishes authority, forensic integrity establishes confidence in the evidence, and admissibility determines whether it may properly be received by the court.



Fig 1 – Conceptual Framework Cross-Border Acquisition, Digital Forensic Integrity, Authentication, Chain of Custody, and Evidentiary Admissibility

3. METHODOLOGY

3.1. Research Design

This study adopts a qualitative comparative doctrinal legal research design to examine the acquisition, preservation, forensic examination, authentication, and admissibility of digital evidence in cross-border cybercrime investigations. The methodology combines analysis of legal rules with

structured comparison of evidentiary, procedural, and digital-forensic requirements across the selected jurisdictions. This approach is appropriate because cross-border digital evidence involves interconnected questions of forensic reliability, jurisdiction, international cooperation, and evidentiary law (Casino et al., 2022; James & Gladyshev, 2016; Zhang & Gong, 2024).

The study does not employ experimental or statistical methods. Instead, it analyses legislation, judicial decisions, international instruments, official guidance, and relevant scholarly literature. Technical digital-forensic literature is additionally examined to evaluate forensic imaging, hashing, metadata, logs, timestamps, encryption, tool validation, cloud acquisition, and chain-of-custody practices relevant to evidentiary reliability (Casey, 2011; Casino et al., 2022; Horsman, 2023). The methodological approach reflects the study's central distinction between lawful acquisition, forensic integrity, and courtroom admissibility.

3.2. Comparative Doctrinal Legal Research Approach

The doctrinal component examines the content and application of legal rules governing electronic evidence, investigative authority, preservation, disclosure, authentication, data protection, and admissibility. Primary legal materials constitute the principal authority, while scholarly literature is used to contextualize and critically examine those rules. The comparative component evaluates each jurisdiction against common legal and forensic dimensions. It does not assume that identical evidentiary rules should operate across different legal systems. Instead, it examines how functionally comparable requirements address the authenticity, integrity, reliability, and lawful acquisition of digital evidence. Such comparison is particularly important because cross-border electronic-evidence frameworks remain fragmented despite increasing international cooperation (Casino et al., 2022; Jerman Blažič & Klobučar, 2020; Zhang & Gong, 2024).

The analysis therefore distinguishes three interconnected questions:

- Was the evidence lawfully obtained?
- Was its forensic integrity adequately preserved and demonstrated?
- Can it satisfy the receiving court's requirements for admissibility?

This distinction is necessary because lawful acquisition through an international cooperation mechanism does not itself establish authenticity, integrity, or admissibility before the receiving court (James & Gladyshev, 2016; Zhang & Gong, 2024).

3.3. Jurisdictional Selection

Five jurisdictions or legal systems are examined: the United Kingdom, European Union, Saudi Arabia, India, and South Africa. The selection is purposive and facilitates comparison between different approaches to digital evidence, cybercrime investigation, cross-border cooperation, and evidentiary admissibility.

The United Kingdom provides an established common-law framework involving criminal evidence, regulated forensic practice, and mechanisms for obtaining electronic evidence internationally. The European Union provides a supranational framework combining mutual-recognition mechanisms with the newer European e-Evidence regime. Regulation (EU) 2023/1543 establishes European Production and Preservation Orders and applies from 18 August 2026 (Regulation (EU) 2023/1543, 2023; Sachoulidou, 2024).

Saudi Arabia is included as a significant Middle Eastern jurisdiction with a distinct framework governing cybercrime, evidence, criminal procedure, electronic transactions, personal-data protection, and international data transfers. Its inclusion broadens the comparison beyond predominantly common-law-influenced systems and enables examination of cross-border evidence within a different legal and regulatory environment.

India provides a major common-law-influenced jurisdiction whose Bharatiya Sakshya Adhiniyam 2023 expressly addresses electronic and digital records, including requirements relevant to proving electronic records (Chadha & Sivaraman, 2024). South Africa provides a further comparative model in which the Electronic Communications and Transactions Act 25 of 2002 and general evidentiary principles influence the admissibility and evidential weight of electronic information (Swales, 2018a, 2018b). The jurisdictions are therefore selected to identify functional similarities and differences rather than to constitute a statistically representative sample.

3.4. Sources of Legal and Documentary Evidence

The study relies primarily on primary legal and official sources, supplemented by peer-reviewed forensic and legal scholarship. Primary materials include national legislation and regulations, judicial decisions, international treaties and protocols, EU regulations and directives, official government guidance, regulatory materials, and documents issued by international organizations.

The international component principally examines the Budapest Convention on Cybercrime and its Second Additional Protocol, together with relevant EU instruments governing cross-border electronic evidence. These mechanisms address preservation, production, international cooperation, and access to electronic evidence across jurisdictions (James & Gladyshev, 2016; Jerman Blažič & Klobučar, 2020).

For Saudi Arabia, primary legal and regulatory materials are used to establish the applicable position concerning cybercrime, electronic evidence, criminal procedure, personal-data protection, and cross-border data transfers. Secondary sources include peer-reviewed journal articles, academic books, and established legal commentary addressing digital forensics, electronic evidence, cloud evidence, jurisdiction, mutual legal assistance, and international cooperation (Casino et al., 2022; Horsman, 2023; Zhang & Gong, 2024). Where secondary literature describes a current statutory rule, the underlying primary authority is checked wherever reasonably available.

3.5. Legal and Comparative Coding Framework

A structured coding framework is used to ensure consistency across the five jurisdictions. The dimensions combine legal requirements with technical forensic considerations identified in digital-forensic and cross-border evidence literature (Casey, 2011; Casino et al., 2022; Horsman, 2023).

Table 1: Comparative Analytical Dimensions of Digital Forensics and Digital Evidence Admissibility

Analytical Dimension	Principal Issue Examined
Legal recognition	Recognition of electronic/digital evidence
Lawful acquisition	Legal authority and procedures for obtaining evidence
Forensic acquisition/imaging	Method used to acquire or image digital data
Preservation	Protection against alteration, deletion, or loss
Hashing/integrity	Verification that acquired evidence remains materially unchanged
Metadata/logs/timestamps	Preservation and interpretation of contextual digital information
Authentication	Establishing identity, origin, and provenance
Reliability/tool validation	Reliability of systems, forensic tools, and analytical methods
Chain of custody	Documentation and continuity of evidence handling
Cloud evidence	Remote, distributed, and provider-controlled evidence
Encryption/access	Effect of encryption and technical access restrictions
Cross-border access	Mechanisms for obtaining evidence internationally
Provider cooperation	Role and obligations of service and cloud providers
Judicial oversight	Authorization, review, and procedural safeguards
Privacy/data protection	Privacy, transfer, and fundamental-rights requirements
Admissibility	Conditions governing courtroom use and evidentiary weight

The framework recognizes that forensic integrity involves more than preservation alone. Reliable digital-forensic examination also depends on defensible acquisition procedures, integrity verification, documentation, reproducibility, and appropriate forensic methods (Casey, 2011; Horsman, 2023). Chain-of-custody documentation is particularly important where evidence passes between service providers, foreign authorities, forensic laboratories, investigators, and courts (Burri et al., 2020; Turner, 2005).

3.6. Data Extraction and Analysis

Relevant information is extracted from each source and organized according to the analytical dimensions established above. For legislation and judicial authorities, attention is given to electronic-evidence recognition, investigative authority, preservation, authentication, cross-border disclosure, procedural safeguards, and admissibility.

For digital-forensic sources, information is extracted concerning forensic acquisition and imaging, hashing, metadata, logs, timestamps, encryption, tool validation, documentation, reproducibility, cloud evidence, and chain-of-custody procedures. These factors are important because digital evidence must remain capable of verification throughout its evidentiary lifecycle (Casey, 2011; Casino et al., 2022; Horsman, 2023). The analysis proceeds in three stages. First, each jurisdiction is

examined independently. Second, corresponding legal and forensic requirements are compared across the five jurisdictions. Third, areas of convergence, divergence, procedural difficulty, and potential interoperability are identified.

The resulting analytical sequence is:

Lawful Acquisition → Forensic Integrity → Courtroom Admissibility

This sequence prevents successful access to electronic information from being treated as equivalent to successful evidentiary use, an important distinction in cross-border investigations (James & Gladyshev, 2016; Jerman Blažič & Klobučar, 2020; Zhang & Gong, 2024).

3.7. Reliability and Source Verification

Source reliability is addressed through a hierarchical verification process. Primary legislation, regulations, treaties, judicial decisions, and official institutional materials are prioritized over secondary commentary. Current legal propositions are verified against official or authoritative versions wherever available.

Particular attention is given to legislative changes occurring during the study period and to differences between legislation that has been enacted and provisions that are actually applicable or in force. This is particularly important for rapidly developing electronic-evidence frameworks such as the EU e-Evidence regime (Sachoulidou, 2024; Shurson, 2025). For technical forensic claims, preference is given to established peer-reviewed digital-forensics literature and recognized forensic guidance concerning acquisition, integrity, reproducibility, chain of custody, and methodological reliability (Casino et al., 2022; Horsman, 2023).

3.8. Ethical and Methodological Considerations

The study relies exclusively on publicly available legal, institutional, and scholarly materials and does not involve human participants, interviews, confidential datasets, or experimental intervention. Consequently, participant consent and confidentiality requirements associated with empirical human-subject research do not arise. Several methodological limitations nevertheless remain. Digital-evidence legislation and international cooperation mechanisms continue to evolve; terminology differs between jurisdictions; reported case law is uneven; and doctrinal analysis cannot independently determine how consistently legal and forensic standards are implemented in operational investigations.

The study also does not experimentally test forensic software or independently validate individual forensic tools. References to tool validation therefore concern the importance of using demonstrably reliable and appropriately documented forensic methods rather than an empirical comparison of particular software products. Tool reliability and methodological transparency remain relevant because the evidentiary value of forensic findings can depend on whether the procedures used to obtain them can be explained, assessed, and reproduced (Horsman, 2023; Ismail & Zainol Ariffin,

2025). These limitations are addressed through consistent comparative criteria, prioritization of primary sources, separation of legal requirements from forensic best practice, and explicit distinction between lawful acquisition, technical integrity, and judicial admissibility.

4. INTERNATIONAL AND TRANSNATIONAL LEGAL FRAMEWORK

Cross-border cybercrime investigations operate within a layered legal environment comprising international treaties, mutual legal assistance arrangements, regional instruments, domestic investigative powers, and mechanisms for cooperation with private service providers. These frameworks seek to facilitate access to electronic evidence while respecting territorial sovereignty, privacy, data protection, procedural legality, and fundamental rights (Casino et al., 2022; James & Gladyshev, 2016).

The increasing use of cloud services adds another dimension to this problem because relevant evidence may be remotely accessible, distributed across several locations, or controlled by a provider in a jurisdiction different from that of the investigator or user. International cooperation mechanisms therefore address not only access to evidence but also its timely preservation and lawful disclosure. For the purposes of this study, however, lawful international acquisition is only the first stage of the evidentiary process. Evidence obtained through a valid cross-border mechanism must still be authenticated and its forensic integrity, provenance, reliability, and chain of custody established before courtroom use.

4.1. Budapest Convention on Cybercrime

The Budapest Convention provides the principal multilateral framework for international cooperation concerning cybercrime and electronic evidence. It establishes substantive criminal-law provisions, procedural powers, and mechanisms for international cooperation relevant to securing electronic evidence (Casino et al., 2022).

Of particular importance are mechanisms concerning expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and mutual assistance. These measures recognize the volatility of digital evidence and the need to preserve relevant data before they are deleted, altered, overwritten, or otherwise become unavailable.

The Convention is particularly relevant to cloud and provider-held evidence because electronic information may be stored in foreign, multiple, shifting, or uncertain jurisdictions. The Council of Europe itself identifies these characteristics as central challenges for cross-border electronic-evidence investigations. Nevertheless, the Convention primarily facilitates the legal acquisition and preservation of evidence. It does not eliminate the need to establish authenticity, integrity, reliability, and compliance with the evidentiary requirements of the court in which the material is ultimately presented.

4.2. Second Additional Protocol

The Second Additional Protocol to the Budapest Convention was developed to strengthen cooperation and disclosure mechanisms for electronic evidence. It provides mechanisms concerning direct cooperation with service providers and domain-name registrars, government-to-government cooperation, emergency cooperation, and other forms of international assistance, accompanied by data-protection and rule-of-law safeguards.

Direct provider cooperation is particularly significant for cloud investigations because relevant subscriber information and other electronic evidence may be controlled by private companies rather than physically possessed by investigative authorities. The Protocol therefore reflects a broader transition from exclusively state-to-state evidence requests toward mechanisms involving direct interaction with private entities (Davies & Kennedy-Mayo, 2026).

However, provider disclosure introduces forensic questions beyond legal authorization. Investigators may need to establish how the provider extracted the information, what metadata accompanied it, whether logs and timestamps were preserved, whether the production was complete, and how integrity was maintained after receipt.

Accordingly, direct disclosure should not be treated as proof of forensic authenticity merely because it was lawfully obtained. A current-status point should also be handled carefully in the paper. The Protocol was opened for signature on 12 May 2022, and implementation and ratification continue to develop. For example, the Council of Europe reported that Hungary became the third state to ratify it in February 2026. Therefore, we should avoid wording that incorrectly suggests universal application.

4.3. Mutual Legal Assistance

Mutual legal assistance (MLA) remains an important mechanism through which one state requests investigative or evidentiary assistance from another. It provides a formal channel for obtaining evidence where domestic investigative powers cannot lawfully be exercised directly in a foreign jurisdiction (James & Gladyshev, 2016). MLA may provide important safeguards concerning sovereignty, legality, and governmental oversight. However, traditional procedures can be poorly suited to highly volatile digital evidence because electronic information may be deleted or overwritten before a request is processed (James & Gladyshev, 2016; Jerman Blažič & Klobučar, 2020).

This difficulty is especially significant for cloud logs, temporary account information, access records, and other provider-held data subject to limited retention periods. Preservation mechanisms are therefore critical while the formal process for production or disclosure proceeds. MLA also does not resolve every forensic issue. Evidence received from a foreign authority must still be documented sufficiently to demonstrate its origin, handling history, integrity, and relationship to the relevant system or account.

4.4. Preservation of Electronic Evidence

Preservation is particularly important because digital evidence may be volatile, remotely stored, automatically overwritten, or subject to provider retention policies. Preservation mechanisms seek to secure relevant information while appropriate legal authority for its production or disclosure is obtained.

In forensic terms, preservation extends beyond preventing deletion. It may require maintaining relevant metadata, system and application logs, timestamps, account information, integrity information, and contextual records necessary to interpret the evidence accurately. Cloud environments make preservation more difficult because investigators may not control the underlying infrastructure. In such cases, the service provider may play a substantial role in preserving relevant information. Preservation should therefore be distinguished from production. Preserving data prevents its loss; it does not itself authorize disclosure or establish admissibility.

4.5. Cross-Border Production and Disclosure

Cross-border production mechanisms permit authorities, subject to applicable legal requirements, to obtain electronic evidence controlled outside their immediate territorial jurisdiction. The EU framework provides an important contemporary example. Regulation (EU) 2023/1543 enables competent authorities to issue European Production Orders and European Preservation Orders to designated establishments or legal representatives of service providers offering services in the Union, subject to the Regulation's requirements. Importantly, the Regulation applies regardless of the location of the relevant data. The Regulation has applied since 18 August 2026, making it directly relevant to the temporal scope of this study. Production nevertheless remains conceptually separate from forensic verification. Once information has been disclosed, investigators must still preserve its provenance and integrity and document how the evidence moved from the provider to investigative authorities and subsequently through forensic examination.

4.6. Service-Provider Cooperation and Cloud Evidence

Private service providers increasingly occupy a central position in cross-border investigations because they may control account information, communications, cloud-stored files, access records, subscriber information, IP logs, and other evidentiary material.

The Second Additional Protocol and EU e-Evidence framework reflect this increasing reliance on provider cooperation. The Council of Europe has specifically identified cooperation with service providers as a central component of the Second Additional Protocol.

From a forensic perspective, provider-produced evidence creates several practical questions. Investigators should be able, where relevant, to determine:

- what data were requested and supplied;
- the relevant account or system from which they originated;
- the method and time of extraction;

- whether metadata and logs were preserved;
- how timestamps should be interpreted;
- whether integrity information was supplied; and
- how the evidence was stored and handled following disclosure.

These considerations become particularly important where investigators cannot independently create a conventional forensic image of the underlying cloud infrastructure.

4.7. Data Protection, Privacy and Fundamental Rights

Cross-border electronic-evidence mechanisms must balance investigative effectiveness against privacy, personal-data protection, procedural fairness, and other fundamental rights. The EU e-Evidence Regulation expressly preserves obligations concerning fundamental rights, including privacy, personal-data protection, freedom of expression, and effective judicial protection. The Second Additional Protocol similarly incorporates human-rights, rule-of-law, and data-protection safeguards.

These safeguards demonstrate that efficient evidence acquisition cannot be evaluated solely according to speed or technical accessibility. Investigative authorities must also establish an appropriate legal basis, comply with applicable authorization and proportionality requirements, and respect relevant restrictions governing disclosure and international transfer. This issue will become especially important in the Saudi Arabian analysis because Saudi Arabia has its own data-protection and cross-border transfer framework.

4.8. Sovereignty and Extraterritorial Access

Digital evidence challenges traditional territorial concepts because data may be stored in one jurisdiction, controlled by a provider in another, accessed by a user elsewhere, and sought by investigators in a fourth jurisdiction (Daskal, 2015; Woods, 2016). Cloud computing intensifies this difficulty because the precise physical location of particular data may be unknown or may change over time. Remote technical accessibility therefore does not necessarily establish lawful investigative authority. States must distinguish between the technical ability to access data and the legal authority to acquire it. Direct access to foreign-hosted or foreign-controlled information may raise sovereignty, jurisdiction, privacy, and procedural concerns even where investigators possess the technical means to obtain it.

International and regional cooperation mechanisms attempt to reduce these conflicts by providing lawful channels for preservation and disclosure. Yet those mechanisms address primarily the acquisition stage. Once evidence is obtained, its forensic integrity, provenance, chain of custody, authenticity, and reliability remain separate evidentiary questions.

Table 2: Principal International and Transnational Legal Instruments Governing Cross-Border Digital Evidence

Instrument / Mechanism	Scope and Purpose	Key Cross-Border Evidence Mechanisms	Principal Relevance to Forensic Integrity and Admissibility
Budapest Convention on Cybercrime	Multilateral framework addressing cybercrime, procedural investigative powers, and international cooperation concerning electronic evidence	Expedited preservation, production orders, search and seizure of stored computer data, mutual assistance, and international cooperation	Facilitates lawful preservation and acquisition, but does not by itself establish authenticity, integrity, chain of custody, or admissibility before the receiving court
Second Additional Protocol to the Budapest Convention	Enhances international cooperation and disclosure of electronic evidence, particularly involving service providers and competent authorities	Direct cooperation with service providers and registrars, enhanced government-to-government cooperation, emergency procedures, and safeguards	Improves access to provider-held and cloud-related evidence, while requiring attention to provenance, metadata, disclosure procedures, integrity, and subsequent evidence handling
EU e-Evidence Framework	EU framework for obtaining electronic evidence from service providers in criminal proceedings	European Production Orders and European Preservation Orders under Regulation (EU) 2023/1543; designated establishments and legal representatives under Directive (EU) 2023/1544	Facilitates cross-border preservation and production of provider-held data. Regulation (EU) 2023/1543 applies from 18 August 2026. Production does not itself determine courtroom admissibility, which remains subject to applicable evidentiary law
Traditional Mutual Legal Assistance (MLA)	Formal state-to-state mechanism for requesting investigative assistance and evidence located or controlled abroad	Requests through competent or central authorities, preservation, collection, production, and transmission of evidence under applicable treaties and domestic law	Supports sovereignty and procedural legality but may be slower for volatile digital evidence. Evidence still requires appropriate documentation of provenance, integrity, transfer, and chain of custody

Source: Authors' synthesis based on the Budapest Convention on Cybercrime, Second Additional Protocol, Regulation (EU) 2023/1543, Directive (EU) 2023/1544, and relevant literature on cross-border electronic evidence.

5. DIGITAL FORENSICS AND EVIDENTIARY ADMISSIBILITY IN THE UNITED KINGDOM

The United Kingdom's framework for digital evidence combines domestic investigative powers, evidentiary and disclosure rules, forensic-quality standards, and international cooperation

mechanisms. Cross-border investigations require UK authorities not only to establish lawful authority to obtain electronic evidence but also to preserve its provenance, integrity, reliability, and continuity for subsequent criminal proceedings. The discussion principally focuses on England and Wales, particularly where the relevant forensic regulatory framework is jurisdiction-specific. The current manuscript already adopts this delimitation, which should be retained.

5.1. UK Cybercrime and Digital-Evidence Framework

The UK does not rely on a single statute governing digital evidence. Relevant rules instead arise from criminal, investigative, evidentiary, forensic, data-protection, and international-cooperation frameworks. Important legislation includes the Computer Misuse Act 1990, Police and Criminal Evidence Act 1984 (PACE), Criminal Procedure and Investigations Act 1996 (CPIA), Criminal Justice Act 2003, Investigatory Powers Act 2016, Forensic Science Regulator Act 2021, and Crime (Overseas Production Orders) Act 2019.

PACE and its Codes regulate important police investigative powers and safeguards, including powers concerning searches and seizure of property. The Forensic Science Regulator Act 2021 adds a statutory quality dimension to forensic science in England and Wales. Version 2 of the statutory Code of Practice came into force on 2 October 2025 and establishes quality-standard requirements for forensic science activities used in criminal investigations and the criminal justice system. Together, these mechanisms illustrate the distinction central to this study: legal authority determines whether evidence may be obtained, while forensic procedures help establish whether the resulting material can subsequently be demonstrated to be authentic, intact, and reliable.

5.2. Relevant Legislative and Forensic Framework

PACE provides an important domestic framework for searches, seizure, and investigative activity. For digital investigations, the exercise of these powers may result in the acquisition of computers, mobile devices, storage media, and other sources containing potentially relevant electronic information. The CPIA provides the principal disclosure framework for criminal investigations and prosecutions. Its significance increases in digital investigations because forensic examinations may generate substantial quantities of potentially relevant electronic material.

The Forensic Science Regulator Act 2021 and statutory Code of Practice provide a further layer concerned with forensic quality. The Code is designed to promote accurate and reliable forensic science and reduce the risks associated with deficient methods and quality failures. This is particularly relevant to digital forensics, where reliability may depend upon acquisition procedures, validated methods, competent examination, appropriate documentation, and quality assurance. The Crime (Overseas Production Orders) Act 2019 is particularly important to cross-border investigations. It enables applications for judicial orders requiring persons overseas to produce or provide access to stored electronic data where the statutory conditions and relevant designated international cooperation arrangements are satisfied.

5.3. Collection, Forensic Acquisition and Preservation

Digital evidence may originate from computers, mobile devices, removable media, communications systems, network infrastructure, online accounts, cloud platforms, and service providers. The method of acquisition should therefore correspond to the characteristics of the source and the investigative purpose.

Where appropriate, forensic acquisition may involve physical or logical extraction, forensic imaging, targeted collection, network capture, or provider-supplied data. Forensic imaging can preserve a reproducible representation of digital material for subsequent examination, while logical acquisition may be necessary where physical acquisition is unavailable or disproportionate (Casey, 2011; Kyei et al., 2013).

Integrity verification is also important. Cryptographic hashing can assist in demonstrating whether acquired digital content remains unchanged between collection and subsequent examination. Hash values should, however, be considered alongside documentation, secure storage, access controls, and chain-of-custody records rather than treated as independent proof of overall evidentiary reliability (Burri et al., 2020; Turner, 2005). Preservation should additionally extend to relevant metadata, system and application logs, timestamps, account information, and other contextual information where those materials are necessary to establish provenance or interpret the evidence accurately.

5.4. Authentication, Metadata and Evidentiary Reliability

Authentication concerns whether digital material can be shown to be what it is represented to be. Relevant evidence may include witness testimony, system information, metadata, account records, forensic documentation, logs, timestamps, and evidence concerning the process through which the information was generated or acquired.

Metadata and logs can be particularly important in reconstructing digital activity, but they require contextual interpretation. A timestamp, for example, may be affected by system configuration, time zones, clock synchronization, application behaviour, or the manner in which data were exported. Investigators should therefore avoid treating individual metadata fields as automatically conclusive. Historically, computer-generated evidence was addressed by section 69 of PACE, but those statutory requirements were subsequently repealed. Contemporary evaluation therefore does not depend on the former computer-operating-condition certification regime.

Reliability remains particularly important where expert forensic evidence is presented. The evidentiary assessment may consider the methodology employed, its scientific or technical basis, documentation of the examination, and whether the conclusions are adequately supported. The statutory forensic framework reinforces this focus on reliable forensic methods and quality assurance. Accordingly, authentication, integrity, reliability, and evidentiary weight are related but should not be treated as identical concepts.

5.5. Chain of Custody, Tool Validation and Forensic Integrity

Chain of custody concerns the documented continuity of evidence from acquisition through preservation, examination, transfer, storage, and courtroom presentation. For digital evidence, appropriate records may identify the source of the material, acquisition date and time, examiner, acquisition method, forensic tools and versions used, hash values, storage arrangements, transfers, access, and significant analytical actions (Casey, 2011; Horsman, 2023).

Tool reliability is similarly relevant. Digital-forensic findings should be produced through methods and tools appropriate to the forensic task, with validation and quality assurance applied where required. Documentation should be sufficient to explain how results were generated and, where practicable, permit another suitably qualified examiner to evaluate or reproduce the process (Horsman, 2023).

These considerations become especially important where evidence moves between investigators, forensic laboratories, service providers, prosecutors, or foreign authorities. Each transfer can create an additional point at which provenance or continuity may later be questioned. Importantly, forensic quality and admissibility are not synonymous. Deficiencies in forensic procedure may affect reliability or evidentiary weight, but the legal consequence depends on the applicable evidentiary rules and judicial assessment.

5.6. Cross-Border Evidence Acquisition and Overseas Production Orders

The Crime (Overseas Production Orders) Act 2019 provides a specific mechanism through which UK authorities can seek stored electronic data from persons located overseas. The legislation was developed partly because substantial amounts of electronic information relevant to UK investigations may be managed, processed, or stored by companies outside the UK.

An overseas production order can require production of, or access to, specified electronic data where statutory requirements are satisfied and the relevant international cooperation arrangement permits the mechanism. The legislation provides that the production requirement may apply regardless of where the electronic data are stored, subject to statutory restrictions. This is particularly relevant to cloud evidence because the physical storage location may differ from the location of the provider, account holder, investigator, or alleged offence.

However, an overseas production order addresses principally the legal acquisition of electronic data. Once the information is produced, separate forensic questions remain concerning its provenance, completeness, metadata, timestamps, integrity, subsequent storage, and chain of custody. The legislation itself recognizes the evidentiary dimension. Its explanatory materials state that, in relevant cases, a judge must have reasonable grounds for believing that the requested material is likely to constitute relevant evidence. Nevertheless, lawful production should not be equated automatically with final courtroom admissibility.

5.7. Cloud and Service-Provider Evidence

Cloud evidence presents particular forensic difficulties because investigators may not have physical access to the underlying servers or storage infrastructure. Evidence may instead be supplied through provider disclosure systems, account exports, remote interfaces, or other provider-controlled mechanisms.

Relevant cloud evidence may include stored communications, files, subscriber information, IP records, authentication records, access logs, audit trails, account metadata, and timestamps. In such circumstances, investigators may be unable to create a conventional bit-for-bit forensic image of the provider's complete infrastructure. The forensic emphasis consequently shifts toward documenting what was requested, what the provider supplied, the source account or system, the method of production, associated metadata, relevant timestamps, integrity information, and subsequent handling.

Encryption can create an additional barrier where data are technically inaccessible despite investigators possessing lawful authority to obtain them. This illustrates an important distinction between legal authority, technical accessibility, and evidentiary usability. The Overseas Production Orders framework is relevant because it was specifically designed to facilitate access to electronic data held by overseas service providers under qualifying international cooperation arrangements.

5.8. Mutual Legal Assistance and Post-Brexit Cooperation

Mutual legal assistance remains an important mechanism where foreign governmental assistance is required or where a direct production mechanism is unavailable. MLA protects sovereignty by allowing evidence to be requested through established international procedures, but its multiple procedural stages may create difficulties where digital evidence is volatile or subject to short retention periods (Casino et al., 2022; James & Gladyshev, 2016).

The UK Government's explanatory material for the Overseas Production Orders legislation similarly recognizes that traditional MLA may not always provide sufficiently rapid access to overseas electronic evidence. Following Brexit, UK-EU criminal-justice cooperation no longer operates on the same basis as cooperation between EU Member States. Consequently, the EU e-Evidence framework should not be presented as though European Production Orders automatically constitute a UK domestic production mechanism.

For this study, the important point is that different acquisition channels may establish lawful access to electronic information, but the resulting material must still satisfy the forensic and evidentiary requirements applicable to its subsequent use.

5.9. Judicial Treatment and Admissibility of Digital Evidence

The treatment of electronic evidence in England and Wales is governed by general evidentiary principles together with rules applicable to particular forms of evidence, expert testimony, and forensic

practice. Digital evidence should therefore not be described as automatically admissible merely because it exists in electronic form or was obtained through a lawful investigative mechanism.

Courts may need to consider provenance, authenticity, integrity, reliability, the circumstances of acquisition, and, where relevant, the methodology underlying expert forensic analysis. Forensic documentation, hash verification, metadata, system records, chain-of-custody evidence, and examiner testimony may contribute to that assessment depending on the nature of the evidence. The statutory forensic regime reinforces the relationship between forensic quality and evidentiary reliability. The current Code establishes quality requirements for forensic science activities in England and Wales and seeks to ensure that accurate and reliable scientific evidence is used within criminal investigations and trials.

The central proposition is therefore:

Lawful acquisition does not automatically establish admissibility. An overseas production order, warrant, or international cooperation mechanism may establish authority to obtain evidence, while authentication, integrity, forensic reliability, procedural compliance, and evidentiary weight remain matters requiring separate consideration.

5.10. Key Challenges within the UK Framework

Several challenges remain significant.

First, cloud and distributed storage weaken simple territorial assumptions because the investigator, user, provider, and underlying data may be connected to different jurisdictions (Daskal, 2015; Svantesson, 2017).

Second, provider-controlled acquisition can limit an investigator's ability to independently image the original infrastructure, increasing the importance of provider records, metadata, production documentation, and provenance.

Third, encryption and rapidly changing technologies may restrict technical access even where lawful authority exists.

Fourth, metadata, logs, and timestamps can provide important evidence of digital activity but require careful interpretation and preservation.

Fifth, forensic tool validation and quality assurance remain important to demonstrating that analytical results are sufficiently reliable. The current statutory Code specifically establishes quality requirements for forensic science activities in England and Wales.

Finally, cross-border acquisition remains dependent upon the interaction of UK law with international cooperation arrangements and the laws of other jurisdictions. The Overseas Production

Orders Act itself operates through designated international cooperation arrangements rather than creating unrestricted unilateral access to overseas electronic evidence.

Overall, the UK framework demonstrates the three-stage relationship central to this study:

Lawful Acquisition → Forensic Integrity → Courtroom Admissibility

The UK possesses mechanisms for obtaining domestic and overseas electronic evidence and a statutory forensic-quality framework. Nevertheless, neither lawful acquisition nor technical integrity independently determines admissibility. Reliable courtroom use depends on their interaction with authentication, procedural safeguards, forensic documentation, and the applicable rules of evidence.

6. DIGITAL FORENSICS AND EVIDENTIARY ADMISSIBILITY IN THE EUROPEAN UNION

6.1. EU Cybercrime and Electronic-Evidence Framework

The European Union has developed a multi-layered framework for obtaining and exchanging electronic evidence in criminal proceedings. It combines Member State criminal-procedure and evidence laws with EU instruments governing judicial cooperation, electronic evidence, data protection and fundamental rights. The framework increasingly supplements traditional mutual legal assistance with more standardized mechanisms for cross-border evidence acquisition, particularly the European Investigation Order (EIO) and the 2023 e-Evidence package (Sachoulidou, 2024; Tosza, 2020).

A central distinction nevertheless remains between obtaining electronic evidence lawfully and establishing its forensic and evidentiary reliability. EU instruments can provide authority for preservation, production or transfer, but they do not eliminate the need to demonstrate provenance, authenticity, integrity and compliance with the evidentiary rules applicable before the receiving court.

6.2. European Investigation Orders

Directive 2014/41/EU established the European Investigation Order as a mutual-recognition mechanism through which a judicial authority in one Member State may seek investigative measures in another Member State for the purpose of obtaining evidence. An EIO may also be used to obtain evidence already held by competent authorities in the executing State.

The EIO therefore provides an important mechanism where digital evidence requires investigative action in another Member State. However, electronic evidence presents particular challenges because data may be volatile, remotely stored or controlled by multinational service providers. Multiple authorities and procedural stages may also complicate timely preservation and acquisition (Casino et al., 2022; Jerman Blažič & Klobučar, 2020). The EIO consequently addresses the legal pathway for obtaining evidence but does not itself establish that the resulting digital material is authentic, complete or forensically reliable.

6.3. Regulation (EU) 2023/1543 on European Production and Preservation Orders

Regulation (EU) 2023/1543 represents a significant development in EU cross-border electronic evidence acquisition. It establishes European Production Orders and European Preservation Orders that may be directed to qualifying service providers offering services within the Union. Importantly, the Regulation permits such orders regardless of the location of the relevant data.

The Regulation applies from 18 August 2026, making it directly relevant to the temporal scope of this study. A European Production Order requires specified electronic evidence to be produced, while a European Preservation Order requires specified data to be preserved for subsequent production. This distinction is particularly important for volatile digital evidence because preservation can prevent deletion or loss while the legal process for obtaining the information continues.

Forensic preservation, however, extends beyond merely retaining the existence of data. Depending on the evidence concerned, subsequent reliability may also depend upon preservation of associated metadata, logs, timestamps, account information and contextual records. Accordingly, lawful preservation and production form part of the evidentiary chain but do not independently establish courtroom admissibility.

6.4. Directive (EU) 2023/1544 and Provider Representation

Directive (EU) 2023/1544 complements the Regulation by establishing harmonized rules requiring relevant service providers to designate establishments or appoint legal representatives through which decisions and orders concerning electronic evidence can be received and enforced. Member States were required to transpose the Directive by 18 February 2026, while service providers already offering services in the Union on that date were required to designate an establishment or appoint a legal representative by 18 August 2026.

The framework is particularly relevant to cross-border cloud investigations because it establishes identifiable points through which authorities can address service providers even where the underlying electronic information is distributed across multiple technical infrastructures. Nevertheless, provider representation primarily facilitates lawful access and enforcement. Separate forensic measures remain necessary to establish the provenance and integrity of the evidence ultimately produced.

6.5. Service-Provider Cooperation and Cloud Evidence

The EU e-Evidence framework reflects the increasingly central role of private service providers in criminal investigations. Relevant providers may control communications, stored files, subscriber information, IP records, account information, access logs and other data potentially relevant to criminal proceedings. Regulation (EU) 2023/1543 specifically covers electronic communications services, domain-name and IP-numbering services and certain information-society services involving communication, storage or processing of data.

Cloud evidence creates particular forensic difficulties because investigators may not possess or physically access the infrastructure from which the evidence originates. Data may be distributed, replicated, dynamically processed or remotely accessible across several locations (Daskal, 2015; Casino et al., 2022). Where evidence is supplied directly by a provider, forensic documentation should therefore establish, where relevant, what information was requested, what was supplied, the account or system from which it originated, how and when it was extracted, what metadata accompanied it, and how the material was handled after receipt. This becomes especially important where a conventional forensic image of the underlying cloud infrastructure cannot reasonably be obtained.

6.6. Authentication, Forensic Integrity and Chain of Custody

Lawful acquisition through an EIO or European Production Order does not itself demonstrate the authenticity or forensic integrity of the resulting evidence. Depending upon the evidence source, integrity may be supported through forensic imaging or controlled acquisition, cryptographic hashing, preservation of metadata and logs, documentation of timestamps, secure storage, access controls and chain-of-custody records (Casey, 2011; Burri et al., 2020; Horsman, 2023).

Hashing can assist in demonstrating that acquired digital content has not materially changed after acquisition, but it does not independently establish who created the evidence, whether the original source was reliable or whether acquisition was legally authorized. Similarly, metadata and timestamps can assist authentication and reconstruction but may require interpretation concerning time zones, system clocks, synchronization, export processes and application behaviour. Forensic tools and analytical methods should also be sufficiently reliable and documented to permit evaluation of the processes used to obtain the findings (Horsman, 2023).

Chain of custody is particularly important where evidence passes through multiple entities, such as a cloud provider, foreign authority, investigative agency, forensic laboratory and prosecutor. Documentation of each material transfer helps establish continuity and identify whether unauthorized alteration or access may have occurred (Burri et al., 2020; Turner, 2007).

6.7. Data Protection and Fundamental Rights

Cross-border electronic evidence frequently contains personal or sensitive information. Data protection, privacy, proportionality, defence rights and access to effective remedies therefore form important safeguards within the EU framework. Regulation (EU) 2023/1543 provides affected persons with rights concerning information and effective remedies, while its broader framework incorporates judicial and procedural safeguards.

These safeguards demonstrate that efficiency in obtaining electronic evidence cannot be evaluated exclusively according to speed. Investigative authorities must also consider the legal basis for acquisition, necessity and proportionality, applicable procedural protections and the rights of persons affected. This distinction reinforces the paper's broader argument: technical accessibility does

not itself establish lawful acquisition, and lawful acquisition does not itself establish evidentiary admissibility.

6.8. Cross-Border Cloud Evidence, Remote Access and Encryption

Cloud computing creates a particular challenge for territorial evidence rules because the investigator, account holder, provider and underlying data may all be associated with different jurisdictions. Data may also be replicated or processed across several locations, making physical server location an incomplete basis for determining investigative authority (Daskal, 2015; Svantesson, 2017).

Regulation (EU) 2023/1543 responds partly to this difficulty by permitting qualifying production and preservation orders regardless of where the data are located. This reduces the importance of identifying the precise physical location of every relevant dataset for purposes of the Regulation's ordering mechanism. Nevertheless, cloud evidence creates continuing forensic challenges. Remote collection may depend on provider interfaces, account exports, APIs or provider-generated productions rather than direct physical acquisition. Investigators may consequently have limited visibility into the provider's underlying infrastructure or extraction process.

Encryption presents a related but distinct difficulty. Evidence may be lawfully subject to an investigative measure while remaining technically inaccessible or only partially recoverable because of encryption or access controls. Legal authority to obtain data and technical capacity to access them must therefore be treated separately.

6.9. Judicial Oversight, Procedural Safeguards and Admissibility

Judicial oversight remains an important component of EU electronic-evidence mechanisms. Directive 2014/41/EU defines the EIO as a judicial decision issued or validated by a judicial authority and requires respect for fundamental rights and defence rights. Regulation (EU) 2023/1543 similarly establishes requirements concerning issuing authorities, enforcement, safeguards and remedies.

However, the EU e-Evidence framework should not be presented as establishing one uniform EU-wide law of digital-evidence admissibility. The Regulation principally regulates cross-border production and preservation, while evidentiary assessment continues to interact with the criminal-procedure and evidence laws applicable to the proceedings. This distinction is crucial. Evidence may have been properly produced under an EU cross-border mechanism but still generate disputes concerning authenticity, provenance, completeness, forensic handling, expert methodology or evidentiary weight.

Accordingly:

Lawful EU Production/Preservation → Forensic Verification → National Judicial Assessment

This sequence accurately separates the functions performed by the EU acquisition framework from those performed by forensic examination and domestic evidentiary law.

6.10. Implications of the Post-August 2026 e-Evidence Framework

As of September 2026, Regulation (EU) 2023/1543 is applicable, while Directive (EU) 2023/1544 has established the complementary framework for designated establishments and legal representatives. The framework represents an important move toward more standardized and direct access to provider-held electronic evidence within the EU.

Its significance is particularly evident for cloud investigations because Regulation (EU) 2023/1543 permits production and preservation orders regardless of the location of the data, while Directive (EU) 2023/1544 establishes identifiable provider representatives or establishments for receipt and enforcement of relevant orders.

Nevertheless, faster production does not resolve every evidentiary problem. The resulting material may still require authentication, integrity verification, metadata and timestamp analysis, chain-of-custody documentation and reliable forensic examination before it can be effectively relied upon in criminal proceedings.

The EU framework therefore reinforces the central analytical model developed in this study:

Lawful Acquisition → Forensic Integrity → Courtroom Admissibility

The first stage has become increasingly standardized through EU electronic-evidence mechanisms. The second and third continue to require careful forensic and judicial assessment.

7. DIGITAL FORENSICS AND EVIDENTIARY ADMISSIBILITY IN SELECTED JURISDICTIONS

7.1. Comparative Rationale

Saudi Arabia, India, and South Africa provide three distinct legal approaches to electronic and digital evidence. India has recently modernized its evidence regime through the Bharatiya Sakshya Adhiniyam 2023 (BSA), including detailed provisions concerning electronic and digital records. South Africa's Electronic Communications and Transactions Act 25 of 2002 (ECT Act) expressly addresses data messages and their evidential weight. Saudi Arabia combines cybercrime legislation, criminal-procedure rules, electronic-transactions legislation, data-protection requirements, and a newer statutory framework expressly recognizing digital evidence. The comparison therefore examines each jurisdiction through the same analytical dimensions used throughout this study: lawful acquisition, preservation, authentication, forensic integrity, metadata and logs, chain of custody, cloud evidence, cross-border access, privacy and admissibility.

7.2. Saudi Arabia

7.2.1. Cybercrime and Digital-Evidence Framework

Saudi Arabia's digital-evidence environment is governed by several interacting legal instruments rather than a single comprehensive digital-forensics statute. Important components include the Anti-Cyber Crime Law, Law of Criminal Procedure, Electronic Transactions Law, Personal

Data Protection Law (PDPL) and associated regulations. Saudi Arabia also has a Law of Evidence containing an express chapter on digital evidence.

The Anti-Cyber Crime Law defines concepts including information systems, information networks, data, computers, unauthorized access and cybercrime. It criminalizes conduct involving unauthorized access, interception, alteration, destruction and misuse of computer data and systems. Article 14 also provides for technical assistance to competent security authorities during the detection, investigation and trial of cybercrimes.

For criminal investigations, the Law of Criminal Procedure is particularly important because it establishes rules governing searches, seizures and access to communications. For example, Articles 56–61 regulate access to communications and the handling of seized correspondence and recorded material, including authorization and confidentiality requirements. This creates the first part of the paper's analytical distinction: authority to investigate or seize digital material concerns lawful acquisition, while the subsequent reliability and evidentiary use of that material raise additional forensic and evidentiary questions.

7.2.2. Legal Recognition of Digital Evidence

Saudi Arabia's Law of Evidence contains detailed provisions concerning digital evidence. Article 53 defines digital evidence broadly as evidence derived from data generated, issued, received, stored or communicated digitally and capable of retrieval or presentation in comprehensible form. Article 54 includes digital records, digital documents, digital signatures, digital correspondence, means of communication and digital media. Article 55 gives proof by digital evidence the legal effect accorded to written proof.

Articles 56–64 further address the probative status, verification, presentation and extraction of digital evidence. For example, Article 60 provides for digital evidence to be presented in its original form or through another digital medium, while Article 63 provides that extracts can have the same probative value as the underlying digital evidence to the extent that they correspond to the digital record.

An important limitation must be stated clearly: Article 1 of the Saudi Law of Evidence provides that the Law applies to civil and commercial transactions. It would therefore be inaccurate to present Articles 53–64 as a comprehensive criminal-evidence code automatically governing every cybercrime prosecution. For this article's criminal context, these provisions are better treated as evidence of Saudi Arabia's statutory approach to digital proof, alongside the Law of Criminal Procedure and other applicable criminal rules. That qualification substantially improves the legal accuracy of the manuscript.

7.2.3. *Electronic Records, Authenticity and Integrity*

The Electronic Transactions Law provides an additional legal basis for assessing electronic records. Article 8 addresses when an electronic record may be treated as an original, linking that status to technical conditions capable of ensuring the integrity of the information from the time the record reaches its final electronic form. Article 9 addresses the evidentiary status and reliability of electronic transactions, signatures and records.

Significantly for digital forensics, Article 9 identifies considerations including the method through which an electronic record was created, stored or communicated, the possibility of alteration, the method used to maintain information integrity, and the method used to identify the originator. These concepts correspond closely with forensic concerns surrounding provenance, authenticity and integrity. However, they should not be interpreted as statutory requirements that every Saudi criminal investigation must use a particular forensic-imaging tool or hashing algorithm. Forensic imaging, cryptographic hashing, metadata analysis, log examination and timestamp verification are instead technical methods capable of supporting these evidentiary objectives where appropriate (Casey, 2011; Horsman, 2023).

7.2.4. *Forensic Acquisition and Chain of Custody*

Digital-forensic integrity requires the investigator to be able to explain how evidence moved from its original source to forensic examination and ultimately to the judicial process. Where physical devices are involved, this may require controlled seizure, forensic imaging or extraction, hashing, secure storage and documentation. Where evidence consists of server records, communications or cloud data, acquisition may instead depend upon targeted collection or disclosure by the entity controlling the information.

Saudi criminal procedure contains relevant preservation principles. Article 31 of the Law of Criminal Procedure requires a criminal-investigation officer, in a flagrante delicto situation, to inspect and preserve material traces at the crime scene and document circumstances relevant to discovering the truth. The Law also regulates seized communications and recorded material and restricts access to seized items in specified circumstances.

From a forensic perspective, continuity should additionally be documented through acquisition records, dates and times, persons involved, transfers, storage arrangements, tools and methods used, and integrity-verification information where applicable. This distinction is important: chain of custody should be presented as a forensic and evidentiary continuity requirement, not falsely described as a single codified Saudi statutory checklist for digital evidence.

7.2.5. *Cloud Evidence, Metadata, Logs and Encryption*

Cloud evidence creates particular difficulties in Saudi investigations because relevant information may be controlled by multinational providers or stored and processed across multiple jurisdictions. Potential evidence can include cloud files, emails, subscriber information, authentication

records, IP logs, access histories, audit logs, metadata and communications records. Unlike the examination of a locally seized storage device, investigators may not have physical access to the infrastructure from which provider-held evidence originates.

Consequently, forensic reliability may depend upon documenting the source account or system, the request made to the provider, the method of production, relevant timestamps and metadata, and the handling of the evidence after receipt. Encryption creates a separate technical problem. Investigators may possess lawful authority to obtain particular information while being unable to access its intelligible contents because of encryption or other technical controls. This reinforces the distinction between legal authority to acquire evidence and technical ability to recover and analyse it.

7.2.6. Personal Data Protection and Cross-Border Transfer

Saudi Arabia's Personal Data Protection Law is highly relevant where cross-border investigations involve personal information. Article 29 regulates transfers or disclosures of personal data outside the Kingdom. Among other conditions, transfers must not prejudice national security or the Kingdom's vital interests, and the framework addresses adequate protection and data minimization.

The implementing transfer framework adds important detail. It requires attention to the purpose and legal basis of transfer, the level of protection abroad, appropriate safeguards and, in specified situations, transfer-risk assessment. Appropriate safeguards may include standard contractual clauses, binding common rules and other recognized mechanisms. Of particular relevance to this study, the current transfer framework recognizes circumstances involving public entities where transfer or disclosure is necessary for the investigation or detection of crimes, prosecution of offenders, or execution of penal sanctions, subject to the applicable regulatory framework.

Accordingly, cross-border cloud investigations involving Saudi personal data must be considered not merely as evidence-access problems but also as questions of lawful international data disclosure. Saudi Arabia presents an important contrast with the European Union. It should not be treated as though the EU e-Evidence Regulation applies to it, nor should the manuscript assume that Budapest Convention mechanisms automatically govern Saudi investigations. Instead, the Saudi analysis should focus on applicable domestic investigative powers, international agreements or cooperation channels relevant to the particular case, provider cooperation, and Saudi rules governing disclosure and international transfer.

This creates several potential points of friction in cross-border cases. Evidence obtained lawfully abroad may still require sufficient proof of its source and integrity when relied upon in Saudi proceedings. Conversely, information sought from Saudi-controlled systems may be affected by domestic privacy, disclosure, criminal-procedure and data-transfer requirements. Saudi Arabia therefore reinforces the paper's principal proposition:

Lawful cross-border acquisition does not, by itself, establish forensic integrity or courtroom admissibility.

7.3. India

7.3.1. *Legal Recognition of Electronic and Digital Records*

India substantially revised its evidentiary framework through the Bharatiya Sakshya Adhiniyam 2023, which replaced the Indian Evidence Act 1872 and came into force in 2024. Sections 61–63 provide the principal framework relevant to electronic and digital records. Section 61 prevents an electronic or digital record from being denied admissibility merely because of its electronic or digital character, subject to the statutory framework for proof. Section 63 establishes requirements governing computer output and electronic records. The existing manuscript is therefore correct to treat the BSA, rather than the former Indian Evidence Act, as the primary contemporary evidence legislation.

7.3.2. *Certification, Source Identification and Hashing*

The BSA provides an unusually explicit connection between evidentiary certification and technical integrity. The certificate contained in the Schedule associated with section 63 requires identification of the device or digital-record source. The listed possibilities expressly include computers, storage media, DVRs, mobile devices, servers and cloud sources. It also provides for identifiers such as IMEI, MAC and Cloud ID where applicable.

Significantly, the certificate also requires the hash value of the electronic or digital record and identification of the algorithm used, with listed examples including SHA-1, SHA-256 and MD5, as well as another legally acceptable standard. This provides a direct statutory connection between electronic-evidence proof and technical integrity verification. Nevertheless, hashing should not be overstated. A matching hash can support a conclusion that particular digital content has remained unchanged, but it does not independently prove authorship, lawful acquisition, contextual accuracy or the reliability of the original system.

7.3.3. *Digital-Forensic Integrity*

Indian digital evidence may originate from computers, mobile devices, servers, communications platforms, cloud services, databases, logs and other digital sources. Forensic examination may therefore involve imaging or extraction, hashing, metadata analysis, log examination, timestamp reconstruction and documentation of the tools and methods used. These practices support the broader statutory concern with establishing the source and reliability of electronic records.

Tool validation is also relevant where forensic conclusions depend upon software used to acquire, recover or interpret digital information. The examiner should be able to document the tool and version used, relevant settings, acquisition procedure and significant errors or limitations where those matters affect the reliability of the result (Horsman, 2023).

7.3.4. Cloud and Cross-Border Evidence

The BSA's express inclusion of a cloud source in its section 63 certificate is particularly significant for this study. It recognizes that contemporary electronic evidence may originate from infrastructure outside the direct physical possession of the party relying upon it. Cross-border cloud evidence nevertheless raises additional questions concerning jurisdiction, provider control, international cooperation, metadata preservation, account attribution and foreign disclosure procedures.

Where a provider supplies evidence, investigators may need to document how the information was obtained, what records were supplied, associated metadata, timestamps and the subsequent handling of the material. These issues demonstrate that certification and lawful acquisition remain connected to, but distinct from, forensic reliability.

7.3.5. Evidentiary Challenges

India's comparatively detailed statutory framework creates clearer technical requirements for certain electronic records, but it does not eliminate cross-border difficulties. Potential problems include satisfying certification requirements, obtaining necessary information from foreign service providers, demonstrating the provenance of provider-generated records, preserving metadata and logs, interpreting timestamps, addressing encrypted material, and maintaining evidentiary continuity during international transfer. The Indian framework therefore supports the central argument of this study: formal recognition of electronic evidence does not remove the need to establish its forensic reliability and satisfy the applicable evidentiary requirements.

7.4. South Africa

7.4.1. Electronic Communications and Transactions Framework

South Africa's principal statutory framework for electronic records is the Electronic Communications and Transactions Act 25 of 2002 (ECT Act). The Act remains in force, although it has been amended, including by the Cybercrimes Act 19 of 2020. The ECT Act establishes legal recognition for data messages and contains provisions directly relevant to admissibility and evidential weight.

7.4.2. Admissibility and Evidential Weight

Section 15 of the ECT Act provides that information should not be denied admissibility merely because it takes the form of a data message. The provision also identifies factors relevant to evidential weight, including the reliability of the manner in which the data message was generated, stored or communicated, the reliability of the manner in which its integrity was maintained, and the manner in which its originator was identified.

This means that the South African framework should not be described as imposing a rigid statutory chain-of-custody checklist. Rather, integrity, reliability, origin and surrounding circumstances contribute to the evidentiary assessment. The current manuscript's treatment of section

15 is therefore conceptually sound, but it benefits from being tied more directly to the forensic processes requested by the buyer. The ECT Act is confirmed by the South African Government as Act 25 of 2002.

7.4.3. Forensic Acquisition, Integrity and Authentication

Digital evidence in South African investigations may include computers, mobile-device data, communications, databases, network logs, cloud records and metadata. Where relevant, forensic imaging and controlled acquisition can preserve material for examination, while hashing can support verification that acquired content has not subsequently changed. Metadata, system logs and timestamps can assist in establishing provenance and reconstructing events.

However, these techniques should be described as methods supporting reliability and integrity rather than as requirements expressly imposed in every case by section 15. Authentication may consequently depend upon a combination of technical evidence, testimony, documentation, system information and circumstances demonstrating the origin and reliability of the digital record.

7.4.4. Chain of Custody and Tool Reliability

Chain-of-custody documentation supports the ability to explain how digital material moved from acquisition through examination, storage, transfer and courtroom presentation. Important records may include acquisition dates and times, persons responsible for handling the evidence, hash values, storage and access records, tools and versions used, transfers and analytical procedures.

Where specialist forensic software is used, validation and documentation of the method can strengthen the reliability of the resulting findings. Again, this should be treated as a forensic-quality consideration rather than falsely attributed to section 15 as an express statutory requirement.

7.4.5. Cloud and Cross-Border Evidence

Cross-border cloud evidence creates many of the same practical difficulties identified in the other jurisdictions. Relevant data may be controlled by a foreign service provider, replicated internationally or accessible remotely without the investigator having physical access to the underlying infrastructure.

Investigators must therefore distinguish three questions:

Can the evidence lawfully be obtained? → Can its forensic integrity and provenance be demonstrated? → Can it satisfy South African evidentiary requirements?

Provider-generated exports, logs and account information may require contextual evidence explaining their origin, method of production and subsequent handling. Differences between South African law and the foreign jurisdiction's acquisition and privacy rules may create additional complications.

7.4.6. Evidentiary Challenges

The South African framework's emphasis on reliability and integrity makes forensic methodology directly relevant to evidential weight. Difficulties may nevertheless arise from cloud storage, encrypted information, provider-controlled records, metadata interpretation, rapidly changing technology and cross-border evidence transfer. Accordingly, the existence of a data message and its lawful acquisition do not independently resolve questions concerning its reliability, integrity or evidential weight.

7.5. Comparative Observation

The three jurisdictions recognize digital or electronic evidence but structure their legal treatment differently. Saudi Arabia has statutory provisions expressly recognizing digital evidence and electronic-record integrity, together with cybercrime, criminal-procedure and personal-data frameworks. Care is required because the Saudi Law of Evidence itself states that it applies to civil and commercial transactions, meaning its digital-evidence provisions should not be inaccurately characterized as a complete criminal-evidence code.

India provides comparatively detailed statutory treatment of electronic and digital records under the BSA, including source identification and hash information in the section 63 certificate. South Africa takes a more principles-oriented approach under the ECT Act, emphasizing the reliability of generation, storage or communication, integrity and identification of origin when assessing electronic evidence.

Despite these differences, all three illustrate the same broader evidentiary problem examined in this article:

Lawful Acquisition → Forensic Integrity → Courtroom Admissibility

Cross-border access mechanisms answer primarily the first question. Forensic imaging or acquisition, hashing, metadata and log analysis, timestamp interpretation, tool validation, documentation and chain of custody address the second. The third ultimately depends on the evidentiary and procedural framework applicable before the receiving court.

8. COMPARATIVE ANALYSIS OF DIGITAL-EVIDENCE FRAMEWORKS

The comparison of the United Kingdom, European Union, Saudi Arabia, India and South Africa demonstrates broad recognition of electronic evidence but significant differences in the legal and procedural mechanisms governing its acquisition, authentication, preservation and courtroom use. These differences become particularly important when evidence crosses national boundaries or is obtained from cloud and service-provider infrastructure.

Across the five frameworks, three questions should remain analytically distinct: whether the evidence was lawfully acquired, whether its forensic integrity and provenance can be demonstrated,

and whether it satisfies the admissibility requirements of the receiving legal system. Cross-border cooperation may answer the first question without necessarily resolving the second or third.

8.1. Comparative Legal Recognition of Digital Evidence

All five frameworks provide mechanisms through which electronic information may acquire evidentiary significance, although the legal foundations differ. In England and Wales, digital material is assessed through general evidentiary principles alongside criminal-procedure rules and the statutory forensic-quality framework. The EU combines Member State evidence laws with supranational mechanisms governing cross-border acquisition, particularly Regulation (EU) 2023/1543, which has applied since 18 August 2026 and establishes European Production and Preservation Orders.

India expressly recognizes electronic and digital records under the Bharatiya Sakshya Adhiniyam 2023. Its section 63 framework is particularly significant because the prescribed certificate identifies digital sources including computers, mobile devices, servers and cloud systems and requires hash information.

Saudi Arabia's legal framework expressly addresses digital evidence and electronic records, but an important qualification is necessary. The Saudi Law of Evidence contains detailed provisions concerning digital evidence, while the criminal context must also be examined through the Law of Criminal Procedure, Anti-Cyber Crime Law and other applicable rules. The Law of Evidence should therefore not be treated as a complete criminal-evidence code. South Africa's ECT Act takes a principles-oriented approach. Section 15 prevents electronic form alone from constituting a basis for exclusion and directs attention to factors including reliability, integrity and identification of the originator when evidential weight is assessed.

8.2. Authentication Requirements

Although the terminology and statutory mechanisms differ, authentication across the jurisdictions concerns the ability to establish the origin and identity of digital material. England and Wales rely substantially on provenance, forensic methodology, supporting testimony, system information and other evidence capable of establishing authenticity. India uses a more formal statutory approach for relevant electronic records, including certification and identification of the digital source under section 63 of the BSA. Its certificate expressly accommodates Cloud IDs and other device or source identifiers.

Saudi law recognizes digital evidence and provides rules concerning its evidentiary status in the contexts governed by the Law of Evidence. For criminal investigations, however, authentication should be considered together with applicable criminal-procedure requirements and evidence concerning the origin and handling of the digital material. South Africa focuses on factors such as the reliability of generation, storage or communication, maintenance of integrity and identification of the

originator. Consequently, authentication is not achieved merely by demonstrating that a file or record exists. Provenance remains central.

8.3. Forensic Integrity and Chain of Custody

The five frameworks converge on the importance of reliable handling but differ in the degree to which forensic requirements are formalized. Forensic imaging or controlled acquisition, cryptographic hashing, secure storage, metadata preservation, documentation and continuity records can support evidence that digital material has remained materially unchanged. However, these practices should not be described as identical statutory admissibility requirements across all five jurisdictions.

England and Wales possess a comparatively formalized forensic-quality framework through the Forensic Science Regulator. India creates an unusually direct statutory connection to technical integrity because its section 63 certificate requires a hash value and the algorithm used.

South African legislation expressly makes integrity relevant to evidential weight, while Saudi Arabia's electronic-record framework similarly recognizes integrity-related considerations. Neither should be converted into a fabricated universal statutory requirement for a particular imaging or hashing procedure. Chain of custody is therefore best treated comparatively as a means of demonstrating continuity, provenance and accountable handling, rather than as an identical codified rule in every jurisdiction.

8.4. Metadata, Logs, Timestamps and Reliability

Digital evidence frequently derives meaning from information beyond the principal file or communication. Metadata can identify creation or modification information; system, application and access logs can reconstruct activity; and timestamps can establish temporal relationships.

These artefacts nevertheless require contextual interpretation. Timestamps may be affected by time zones, clock configuration, synchronization, application behaviour and export processes. Logs may be incomplete, automatically overwritten or generated by systems whose operation must itself be understood. Accordingly, reliability depends not only on whether a digital artefact has remained unchanged but also on whether the system, method and context through which it was generated, acquired and interpreted are sufficiently reliable. This issue cuts across all five jurisdictions and demonstrates why forensic integrity cannot be reduced to hashing alone.

8.5. Evidence Preservation Mechanisms

Preservation is critical because electronic information may be deleted, overwritten, remotely altered or lost before formal production procedures are completed. The EU provides an explicit cross-border preservation mechanism through European Preservation Orders under Regulation (EU) 2023/1543. The Regulation allows qualifying orders to require preservation of electronic evidence regardless of the location of the underlying data.

The UK can employ domestic investigative mechanisms, international cooperation and, in qualifying circumstances, overseas production procedures. India, Saudi Arabia and South Africa depend on their applicable domestic investigative procedures and relevant international cooperation mechanisms when evidence is located or controlled abroad. From a forensic perspective, preservation should extend where appropriate to associated metadata, logs, timestamps and contextual information. Preserving a file while losing information necessary to establish its provenance may substantially reduce its evidentiary value.

8.6. Cross-Border Evidence Acquisition

The greatest divergence appears in the mechanisms available for obtaining foreign-held electronic evidence. The UK has the Crime (Overseas Production Orders) Act 2019, under which a qualifying overseas production order can require an overseas person to produce stored electronic data or provide access to it where an applicable designated international cooperation arrangement exists.

Within the EU, Regulation (EU) 2023/1543 permits European Production and Preservation Orders to qualifying service providers offering services in the Union, regardless of where the requested data are physically located. India, Saudi Arabia and South Africa do not have equivalent access to the EU's internal e-Evidence mechanism. Their cross-border investigations may therefore require applicable domestic procedures, provider cooperation, mutual legal assistance, treaties or other international cooperation mechanisms depending on the circumstances.

Saudi Arabia should not be presented as though EU e-Evidence or Budapest Convention mechanisms automatically apply to it. Its applicable international legal basis must be identified separately for the particular cooperation relationship involved.

8.7. Service-Provider and Cloud Cooperation

Service providers occupy a central position because emails, cloud files, subscriber information, IP information, authentication records, access logs and communications may be under private rather than governmental control. The EU has established a structured provider-facing mechanism through Regulation (EU) 2023/1543 and the complementary representation framework. The Regulation expressly applies to electronic evidence held by relevant service providers and operates regardless of the location of the data.

The UK similarly provides a mechanism for direct production from overseas service providers where the Overseas Production Orders Act and an applicable international cooperation arrangement permit it. The UK Government explains that the Act was developed specifically because substantial amounts of electronic information are managed or stored by companies outside the UK. For Saudi Arabia, India and South Africa, provider cooperation depends more heavily on the applicable domestic and international legal mechanisms in the particular investigation. Regardless of jurisdiction, provider-produced evidence creates forensic questions concerning how the data were extracted, whether the

production is complete, what metadata accompanied it, how timestamps were generated and how integrity was maintained after receipt.

8.8. Judicial Authorization and Oversight

Judicial and legal oversight provides safeguards against unauthorized or disproportionate access to electronic information, although the applicable procedures differ substantially. UK Overseas Production Orders require judicial authorization and satisfaction of statutory conditions. EU Production and Preservation Orders similarly operate through specified issuing or validating authorities and associated safeguards.

India, Saudi Arabia and South Africa apply their respective criminal-procedure, constitutional or statutory rules to investigative measures. The comparative significance is therefore not simply whether judicial oversight exists, but which authority must approve a particular measure, what threshold applies, what category of data is sought and what procedural safeguards accompany acquisition.

8.9. Privacy and Data-Protection Safeguards

Cross-border digital-evidence acquisition intersects with privacy and personal-data regulation. The EU combines its electronic-evidence regime with extensive fundamental-rights and data-protection safeguards, including remedies for persons affected by European Production Orders. Saudi Arabia's PDPL and implementing framework are particularly relevant to international disclosure because transfers of personal data outside the Kingdom are subject to specific requirements and safeguards.

The UK, India and South Africa likewise maintain privacy and data-protection frameworks relevant to processing and international transfers. Accordingly, investigators cannot assume that evidentiary relevance alone creates lawful authority to transfer personal information internationally. Evidence law, investigative authority and data-protection law may operate simultaneously.

8.10. Mutual Legal Assistance and International Cooperation

Mutual legal assistance remains significant where a direct production mechanism is unavailable, legally inappropriate or outside the scope of a specialized instrument. Its principal advantage is that evidence is obtained through formal state-to-state cooperation. Its principal difficulty in digital investigations is time. Electronic information may be deleted, overwritten or become unavailable while formal procedures are being completed.

The UK Government itself identifies delays associated with conventional MLA as part of the policy background to the Overseas Production Orders Act. The EU's Production and Preservation Order framework similarly reflects efforts to create more direct mechanisms for obtaining provider-held electronic evidence. The comparison therefore shows a broader movement from exclusive

dependence on traditional MLA toward hybrid models combining state cooperation, expedited preservation and provider-facing mechanisms.

8.11. Cloud Computing, Remote Access and Encryption

Cloud computing weakens the traditional assumption that evidence exists within one identifiable territorial location. The provider, user, investigator and underlying infrastructure may all be associated with different jurisdictions (Daskal, 2015; Woods, 2016). The EU framework addresses this directly by permitting qualifying orders regardless of the physical location of the requested data. The UK's overseas-production framework likewise responds to circumstances in which electronic information relevant to UK investigations is managed, processed or stored by companies abroad.

Cloud acquisition also changes forensic practice. Investigators may have to rely on provider exports, remote interfaces, APIs, account downloads or targeted disclosures rather than conventional physical forensic imaging. Encryption creates an additional distinction. An authority may possess lawful power to obtain data but still be unable to decrypt or interpret it.

Thus:

Legal authority ≠ technical accessibility ≠ forensic reliability ≠ admissibility.

These questions overlap but should not be treated as interchangeable.

8.12. Convergence and Divergence across Jurisdictions

The principal area of convergence is recognition that electronic information can have evidentiary value and that authenticity, integrity, reliability, provenance and procedural legality matter when such information is used in legal proceedings. The principal divergence lies in how these objectives are implemented.

England and Wales combine general evidentiary principles with statutory forensic-quality regulation and specialized overseas-production mechanisms. The EU has developed a regional cross-border production and preservation regime that has applied since 18 August 2026. India provides detailed statutory requirements for proving relevant electronic records, including express hash and source information. Saudi Arabia combines digital-evidence, electronic-transactions, criminal-procedure, cybercrime and personal-data rules, while South Africa places express statutory emphasis on the reliability, integrity and origin of data messages when assessing evidential weight.

The comparison therefore supports the paper's central proposition. Cross-border evidence interoperability cannot be achieved solely by creating faster mechanisms for obtaining data. The evidence must also remain capable of satisfying the forensic and evidentiary expectations of the jurisdiction in which it is ultimately used.

Lawful Acquisition → Forensic Integrity → Courtroom Admissibility

Table 3: Comparative Legal Requirements for Digital-Evidence Admissibility

Jurisdiction	Principal Framework	Legal Recognition	Authentication	Integrity / Chain of Custody	Key Evidentiary Consideration
United Kingdom (England & Wales)	PACE 1984; Criminal Justice Act 2003; Forensic Science Regulator Act 2021 and Code	Digital evidence operates under general evidentiary and procedural principles	Provenance, testimony, forensic methodology and circumstances of acquisition may establish authenticity	Documented acquisition, preservation, secure handling and forensic-quality procedures support integrity	Lawful acquisition and forensic integrity do not automatically determine admissibility
European Union	Member State evidence law; Directive 2014/41/EU; Regulation 2023/1543; Directive 2023/1544	EU instruments facilitate lawful cross-border acquisition; courtroom admissibility remains substantially governed by applicable national law	Source, production process, secure transmission and applicable national evidentiary mechanisms	EU mechanisms protect preservation and subsequent forensic continuity remains important	EU production/preservation mechanisms should not be mistaken for a uniform EU admissibility code
Saudi Arabia	Law of Criminal Procedure; Anti-Cyber Crime Law; Electronic Transactions Law; Law of Evidence; PDPL	Saudi legislation expressly recognizes digital/electronic evidence in relevant legal contexts	Origin, electronic-record characteristics and supporting evidence may establish authenticity	Integrity and reliable electronic-record handling are relevant; forensic continuity should be documented	Law of Evidence provisions must not automatically be treated as a comprehensive criminal-evidence code
India	Bharatiya Sakshya Adhiniyam 2023, particularly ss. 61–63	Express recognition of electronic and digital records	Section 63 certification identifies relevant digital sources	Certificate includes hash value and algorithm, directly supporting technical integrity verification	Compliance with applicable statutory requirements for proving electronic records

South Africa	Electronic Communications and Transactions Act 25 of 2002, particularly s. 15	Electronic form alone is not a basis for exclusion	Identification of originator and surrounding evidence support authentication	Reliability of integrity maintenance is expressly relevant to evidential weight	Reliability, integrity, origin and other relevant circumstances influence evidential weight
--------------	---	--	--	---	---

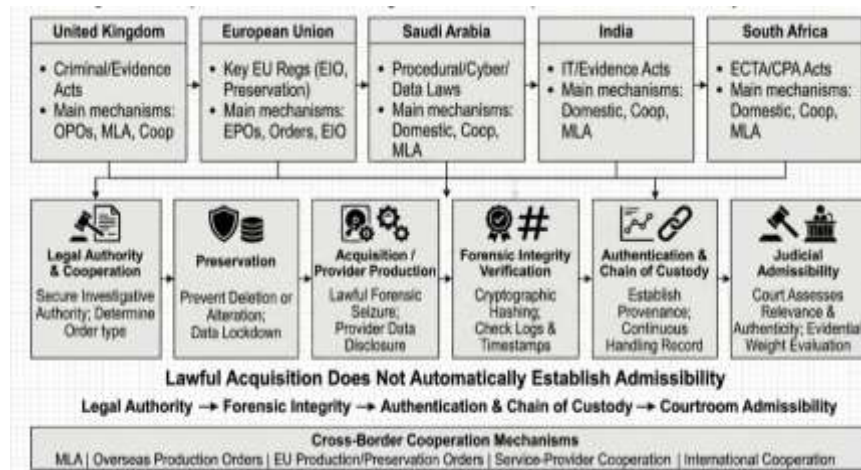


Fig 2 – Comparative Cross-Border Digital-Evidence Acquisition and Admissibility Process

Table 4: Cross-Border Electronic-Evidence Acquisition Mechanisms

Jurisdiction / Framework	Principal Mechanism	Service-Provider Role	Oversight	Principal Cross-Border Limitation
United Kingdom	Overseas Production Orders; MLA; international cooperation arrangements	Qualifying overseas providers may be ordered to produce stored electronic data	Judicial order and statutory conditions	Overseas Production Orders depend on an applicable designated international cooperation arrangement
European Union	European Production Orders; European Preservation Orders; EIO	Providers receive qualifying production/preservation orders through the EU framework	Specified issuing/validating authorities and procedural safeguards	Framework operates within its statutory EU scope; third-country conflicts may require other mechanisms
Saudi Arabia	Domestic investigative powers; applicable international cooperation/MLA mechanisms	Providers may hold cloud, subscriber, communication and log evidence	Applicable Saudi criminal-procedure and other legal requirements	No assumption should be made that EU e-Evidence or Budapest mechanisms automatically apply; applicable cooperation

				basis must be separately established
India	Domestic investigative procedures; MLA and applicable international cooperation	Domestic or foreign providers may control relevant electronic/cloud records	Applicable Indian judicial and statutory procedures	Foreign-held evidence may require international cooperation and compliance with foreign provider/jurisdiction requirements
South Africa	Domestic investigative procedures; MLA and applicable international cooperation	Providers may possess communications, cloud and account records	Applicable South African procedural and statutory requirements	Foreign-held evidence may require cooperation under external legal mechanisms

9. DIGITAL FORENSIC INTEGRITY AND THE ADMISSIBILITY CHAIN

Digital evidence must remain demonstrably reliable from its initial identification through courtroom presentation. This creates an evidentiary chain in which identification, preservation, acquisition, integrity verification, examination, documentation, authentication, custody and judicial assessment are interconnected. A weakness at any stage may affect authenticity, reliability, evidential weight or, depending on the applicable legal framework, admissibility (Casey, 2011; Horsman, 2023).

This section therefore treats forensic integrity as the technical bridge between lawful acquisition and courtroom admissibility. A legal power, production order or international cooperation mechanism may authorize access to evidence, but it does not by itself establish that the material subsequently presented before a court is complete, authentic or forensically reliable.

9.1. Identification of Digital Evidence

The forensic process begins with identifying potentially relevant evidence and determining where it is located or controlled. Sources may include computers, mobile devices, removable media, servers, network infrastructure, databases, emails, messaging platforms, social-media accounts, cloud services, access logs, audit records and associated metadata.

Identification should consider not only relevance but also the location, ownership or control, volatility, accessibility and technical characteristics of the potential evidence. These factors influence both the legal authority required for acquisition and the appropriate forensic method. The distinction is particularly important for cloud evidence. A physical device may permit direct forensic acquisition, whereas remotely stored evidence may require preservation requests, provider production, account exports, APIs or other forms of remote collection. Cross-border investigations should therefore

establish both who controls the evidence and what lawful mechanism permits access to it before forensic acquisition begins (Casino et al., 2022).

9.2. Preservation and Initial Documentation

Preservation aims to prevent the alteration, destruction, overwriting or loss of potentially relevant evidence. Digital information is particularly vulnerable because it may be automatically modified by normal system operations or deleted through retention policies. Investigators should document the source and condition of the evidence, relevant dates and times, persons involved, preservation actions and subsequent handling. Where evidence is controlled by a service provider, an appropriate preservation request or legal order may be necessary before formal production is completed.

Preservation should extend beyond the principal file or communication where contextual information may have evidentiary significance. Relevant metadata, system logs, access records, timestamps, account identifiers and audit information should therefore be preserved where practicable. This is especially important in cloud investigations because preserving the visible content while losing associated provider metadata or access logs may weaken subsequent efforts to establish provenance or reconstruct events.

9.3. Forensic Imaging and Acquisition

Forensic acquisition involves obtaining digital information through methods designed to preserve its evidentiary characteristics and permit subsequent examination. Depending on the source, acquisition may involve bit-stream forensic imaging, physical extraction, logical acquisition, targeted collection, network capture or cloud/service-provider acquisition (Casey, 2011; Kyei et al., 2013).

A forensic image may be appropriate where investigators need a reproducible representation of accessible storage media. Physical extraction may provide access to lower-level device information, while logical acquisition obtains data available through the operating system, application or authorized interface.

Cloud environments require a different approach. Investigators may not have physical access to the underlying storage infrastructure and may instead rely on provider exports, remote interfaces, APIs or data produced pursuant to legal process. In such cases, documentation should establish the source account or system, scope of the request, method of acquisition, date and time of production, associated metadata and subsequent handling. The acquisition method should therefore be selected according to the evidence source rather than assuming that conventional physical imaging is possible in every digital investigation.

9.4. Hashing and Integrity Verification

Cryptographic hashing provides an important mechanism for verifying whether acquired digital content has changed after acquisition. A hash value generated at acquisition can be compared

with values calculated at later stages. Matching values provide strong technical support for the conclusion that the hashed content remains unchanged (Turner, 2005; Burri et al., 2020).

However, hashing proves a limited proposition. A matching hash does not independently establish who created the evidence, whether the original source was reliable, whether the evidence was lawfully obtained, or whether relevant contextual data were omitted during acquisition. Hash verification should therefore operate alongside acquisition documentation, metadata preservation, secure storage, access controls and chain-of-custody records.

Where evidence is supplied by a cloud provider, hashing should also be interpreted according to what was actually hashed. A hash of a provider-produced export can demonstrate the subsequent integrity of that export, but it does not automatically prove that the export represents the complete underlying provider dataset.

9.5. Metadata, Logs and Timestamp Analysis

Metadata and logs are particularly important in reconstructing digital activity and establishing provenance. Relevant metadata may record creation, modification, access or transmission information, while system, network, application, authentication and audit logs may document user or machine activity. Timestamps require particular caution. Apparent chronological inconsistencies may arise from time-zone differences, daylight-saving adjustments, unsynchronized system clocks, application-specific time formats or conversion during data export. Investigators should therefore document the time reference and normalization process used when reconstructing a timeline.

Logs also require contextual evaluation. A log entry may demonstrate that a particular system recorded an event, but its reliability depends partly on the system that generated it, its configuration, retention policy and protection against alteration. Accordingly, metadata, logs and timestamps should be interpreted collectively with other forensic and contextual evidence rather than treated as inherently conclusive.

9.6. Examination, Tool Validation and Reproducibility

Forensic examination involves extracting, recovering, organizing and interpreting relevant information from acquired data. Techniques may include file-system analysis, deleted-file recovery, keyword searching, metadata examination, timeline reconstruction, communication analysis and log correlation.

The reliability of forensic conclusions depends partly upon the methods and tools used. Examiners should therefore document relevant tool names and versions, configuration settings, analytical procedures, errors, limitations and validation information where these matters affect the interpretation of results (Horsman, 2023).

Tool output should not be treated as automatically correct merely because it was generated by forensic software. Where material findings depend on a particular tool or method, validation, independent verification or reproducibility may strengthen confidence in the result. Reproducibility does not necessarily require every examination to be repeated. Rather, documentation should be sufficiently complete to enable another suitably qualified examiner to understand the procedure and, where practicable, reproduce or independently evaluate material findings.

9.7. Authentication and Evidentiary Reliability

Authentication connects technical forensic work to legal proof. It concerns whether evidence can be established as what the party presenting it claims it to be. Depending on the jurisdiction and evidence type, authentication may be supported by witness testimony, metadata, system records, provider records, forensic examination, statutory certificates, hash values or documentation demonstrating how the evidence was generated, acquired and preserved.

Authentication should nevertheless remain conceptually distinct from integrity and reliability. An intact file may have uncertain provenance, while an authenticated record may originate from an unreliable system. Similarly, technically reliable evidence may have been obtained through an unlawful procedure.

The relevant questions are therefore:

What is the evidence? Where did it originate? Has it remained materially intact? Is the process that generated and examined it sufficiently reliable?

These questions become particularly important when evidence crosses jurisdictions with different evidentiary requirements.

9.8. Chain-of-Custody Continuity

Chain of custody documents the history of evidence from acquisition through preservation, examination, transfer, storage and courtroom presentation. Records should identify, where appropriate, the source of the evidence, date and time of acquisition, persons responsible, acquisition method, tools used, hash values, storage arrangements, transfers, access events and significant forensic actions (Turner, 2007; Burri et al., 2020).

Cross-border investigations increase the complexity of this process because evidence may pass through a service provider, foreign authority, law-enforcement agency, forensic laboratory, prosecutor and court. Each transfer can create a potential evidentiary vulnerability. Accordingly, transfer records should establish what was transferred, by whom, to whom, when, through what mechanism and with what integrity information. Chain of custody is therefore not merely administrative record keeping. It provides an evidentiary account connecting the digital material presented before the court with the material originally acquired.

9.9. Cloud Evidence and Cross-Border Transfer

Cloud evidence creates a particularly difficult relationship between acquisition and forensic integrity. Data may be stored, replicated or processed across multiple jurisdictions while remaining under the control of a provider located elsewhere. Investigators may consequently receive evidence that they did not personally extract from the original infrastructure. In such circumstances, provenance becomes especially important.

Documentation should identify, where available, the legal request or production mechanism, provider, relevant account or system, scope of the production, extraction or export method, production date and time, metadata supplied, integrity information and subsequent chain of custody.

Encryption may create an additional barrier. Evidence may be lawfully obtained yet remain technically inaccessible or partially inaccessible. This reinforces the need to distinguish:

Legal Authority → Technical Accessibility → Forensic Integrity → Evidentiary Use

Cross-border transfer also introduces risks of metadata loss, format conversion, incomplete exports and discontinuity in handling. Evidence should therefore be transferred in a manner that preserves both its substantive content and the contextual information necessary for subsequent authentication.

9.10. Judicial Assessment of Digital Forensic Evidence

The final stage is judicial assessment. Depending on the applicable legal system, courts may consider relevance, authenticity, integrity, reliability, provenance, procedural legality, forensic methodology, expert evidence and continuity of custody. A deficiency at one stage does not necessarily produce automatic exclusion in every jurisdiction. Depending on the governing law and circumstances, it may instead affect admissibility, evidential weight or the credibility of the forensic interpretation.

This distinction is central to cross-border digital evidence. A court should be capable of separating questions concerning how evidence was legally obtained, whether its technical integrity was preserved, and whether the evidentiary foundation required by the receiving jurisdiction has been established.

The complete digital-evidence lifecycle examined in this study can therefore be represented as:

Identification → Preservation → Acquisition → Integrity Verification → Examination →
Documentation → Authentication → Chain of Custody → Cross-Border Transfer → Judicial
Assessment

This lifecycle reinforces the paper's central argument. Lawful acquisition is necessary but not sufficient. Digital evidence obtained through a valid domestic or international mechanism may still encounter evidentiary difficulty where provenance is uncertain, metadata has been lost, timestamps

cannot be explained, forensic methods are unreliable, or chain-of-custody documentation is incomplete.

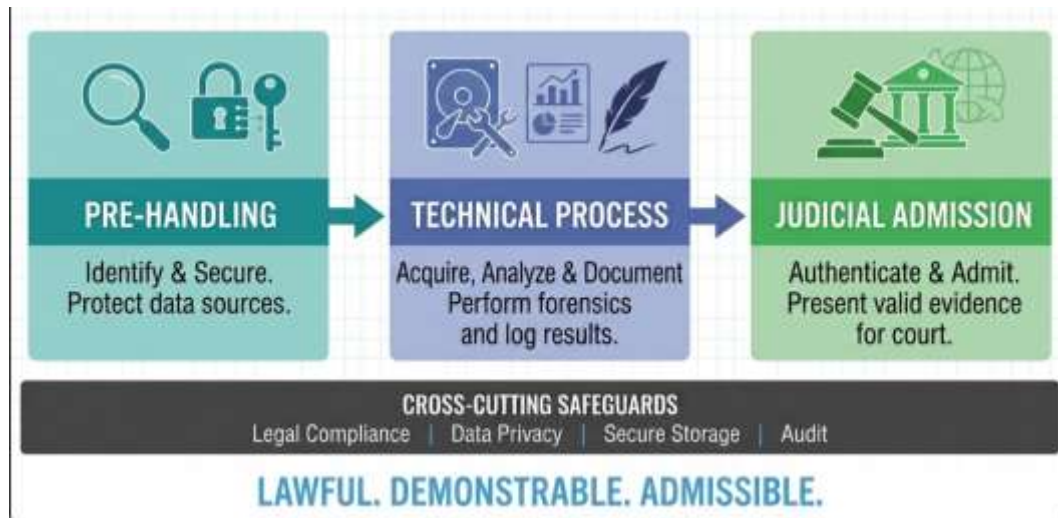


Fig 3 - Digital Forensic Evidence Lifecycle from Acquisition to Judicial Admissibility

10. KEY CHALLENGES IN CROSS-BORDER CYBERCRIME INVESTIGATIONS

Cross-border cybercrime investigations face interconnected legal and technical difficulties because electronic evidence may be volatile, controlled by private providers, or located across several jurisdictions. Cloud computing and jurisdictional uncertainty remain particularly important obstacles to effective international cooperation.

10.1. Jurisdictional Conflicts

Cybercrime frequently involves offenders, victims, infrastructure, and evidence located in different states. Competing jurisdictional claims can therefore create uncertainty over which authority may lawfully obtain or disclose evidence.

10.2. Key Challenges in Cross-Border Cybercrime Investigations

Cross-border cybercrime investigations involve interconnected legal, technical and evidentiary difficulties. Electronic evidence may be distributed across jurisdictions, controlled by private service providers, encrypted, remotely accessible, or subject to rapid deletion. Consequently, investigators must address not only how evidence can be obtained lawfully but also whether its provenance, integrity and reliability can be demonstrated after acquisition.

These challenges are particularly acute in cloud environments, where the physical location of data may have limited correspondence with the location of the user, service provider or investigating authority. The resulting problems affect the entire evidentiary process from preservation and acquisition to authentication and courtroom use (Daskal, 2015; Casino et al., 2022).

10.3. Jurisdictional Conflicts

Cybercrime frequently connects offenders, victims, devices, service providers and digital infrastructure located in different states. More than one jurisdiction may therefore claim authority over the same conduct or evidence.

Traditional territorial rules become difficult to apply where electronic information is remotely accessible or distributed across multiple systems. A provider may be incorporated in one country, operate infrastructure in another, process information in several others and provide services to a user located elsewhere (Daskal, 2015; Woods, 2016). Investigators must consequently distinguish between the location of data, location of the provider, location of the user, control over the data and legal authority to compel its disclosure. Technical ability to access information remotely should not be treated as equivalent to lawful authority to obtain it.

10.4. Data Sovereignty and Cross-Border Transfer Restrictions

National sovereignty remains an important limitation on foreign investigative activity. A state may object to another state's authorities directly searching, extracting or compelling disclosure of information within its jurisdiction without an appropriate legal basis.

Data-protection and localization requirements add another layer of complexity. A service provider may technically possess the ability to disclose requested information but remain subject to domestic restrictions governing international transfer. Saudi Arabia provides a relevant example because its Personal Data Protection Law regulates transfers and disclosures of personal data outside the Kingdom. Cross-border investigations involving Saudi-controlled personal data must therefore consider the applicable transfer framework alongside criminal-investigation requirements. Accordingly, technical control over data does not necessarily create legal authority to transfer it internationally.

10.5. Cloud-Based and Distributed Evidence

Cloud computing creates one of the most significant practical challenges in modern digital forensics. Evidence may be distributed, replicated, dynamically moved or processed across multiple data centres. The investigator may consequently be unable to identify a single physical storage location. Relevant evidence may include emails, documents, messages, cloud backups, virtual-machine data, subscriber information, authentication records, IP logs, access histories, audit trails and associated metadata. Traditional forensic imaging may not be possible where investigators lack physical access to the provider's infrastructure. Instead, evidence may be acquired through provider exports, account downloads, APIs, remote interfaces or legally compelled production.

This changes the forensic question. Rather than simply asking whether a physical device was correctly imaged, investigators may need to establish:

what was requested, what the provider produced, where the information originated, how it was extracted, what metadata accompanied it and how it was preserved after receipt. Provider-

generated evidence may therefore require supporting records explaining the production process and provenance.

10.6. Remote Access and Provider-Controlled Acquisition

Remote access creates a distinct problem from conventional seizure. Investigators may technically be able to access an online account or remote system from their own jurisdiction even though the underlying information is stored or controlled abroad. Such technical accessibility does not resolve whether remote acquisition is legally authorized. The relevant legal framework may require provider cooperation, judicial authorization, mutual legal assistance or another international mechanism.

Provider-controlled acquisition also reduces the examiner's direct control over the initial collection process. The provider may determine the export format, available metadata, retention period and categories of information supplied. Investigators should therefore document the legal request, scope of requested data, provider response, production format, associated metadata, timestamps, integrity information and subsequent forensic handling. This documentation becomes part of the provenance necessary to explain how provider-controlled information entered the evidentiary chain.

10.7. Encryption and Technical Access Barriers

Encryption protects confidentiality, cybersecurity and privacy but can also prevent investigators from accessing relevant content. The central distinction is between legal entitlement and technical accessibility. Investigators may possess a valid warrant, production order or other lawful authority while remaining technically unable to decrypt the information.

Encryption can affect locally seized devices, encrypted communications, cloud storage and provider-held information. In some circumstances, a provider may possess responsive information but lack access to readable content because of the technical architecture of the service. Investigators must therefore avoid assuming that lawful acquisition automatically produces usable evidence. Where encrypted material cannot be accessed, surrounding evidence such as metadata, access records, account information, logs or communications information may remain relevant, subject to the applicable legal framework.

10.8. Volatile Evidence, Logs and Metadata Loss

Digital evidence may be deleted, overwritten or modified rapidly. Volatility is particularly important for logs, temporary files, cloud-session information, IP records and other data subject to short retention periods. Delays in international cooperation can therefore cause relevant information to disappear before formal production occurs (James & Gladyshev, 2016).

Metadata loss presents an additional problem. A file may remain available while contextual information concerning its creation, modification, access, transmission or source has been lost. Prompt preservation should therefore consider not only the principal content but also relevant metadata, logs,

timestamps and account information. This demonstrates why preservation orders and expedited requests are particularly important in cross-border investigations.

10.9. Differences in Authentication Standards

Jurisdictions differ in the mechanisms through which electronic evidence is authenticated. India provides comparatively detailed statutory requirements for specified electronic records, including source information and hash values under the BSA. South Africa expressly considers factors including integrity, reliability and identification of the originator when determining evidential weight. England and Wales rely more heavily on general evidentiary principles together with forensic-quality requirements, while the EU leaves important questions of courtroom admissibility to applicable Member State law.

Saudi Arabia adds a different legal framework involving criminal procedure, electronic transactions and digital-evidence rules applicable within their respective statutory scopes. Evidence obtained properly in one jurisdiction may therefore require additional proof when introduced elsewhere. Cross-border investigators should anticipate the authentication requirements of the receiving jurisdiction during acquisition, rather than attempting to reconstruct the necessary evidentiary foundation only after transfer.

10.10. Chain-of-Custody Discontinuity

Cross-border evidence may pass through service providers, foreign authorities, law-enforcement agencies, forensic laboratories and prosecutors before reaching court. Every transfer creates a potential break in evidentiary continuity. Problems may arise where transfer dates are unclear, access is undocumented, integrity values are unavailable, provider production procedures are unexplained or different agencies maintain incompatible evidence-management records.

A defensible cross-border chain should therefore document, where appropriate, the evidence source, acquisition or production method, persons or entities responsible, relevant timestamps, transfers, storage, access and integrity-verification information. The greater the number of organizations involved, the more important this documentation becomes.

10.11. Privacy and Data-Protection Conflicts

Electronic evidence frequently contains personal information concerning suspects, victims and third parties. Cross-border investigative demands can therefore conflict with privacy, data-protection and fundamental-rights obligations.

The EU e-Evidence framework combines production and preservation mechanisms with procedural safeguards and remedies. Saudi Arabia regulates international personal-data transfers through its PDPL framework. The UK, India and South Africa likewise maintain legal rules governing privacy or personal-data processing. Investigators must therefore consider both authority to obtain evidence and authority to process, disclose or transfer the personal information contained within it.

This interaction may become particularly complicated where the requesting and responding jurisdictions impose different requirements.

10.12. Delays in Mutual Legal Assistance

Traditional mutual legal assistance provides an established state-to-state mechanism for obtaining foreign evidence, but its procedural stages may be slow relative to the volatility of electronic information (James & Gladyshev, 2016). The risk is particularly significant where providers retain certain logs or account records only for limited periods.

This problem has contributed to the development of expedited preservation and more direct production mechanisms. Examples include the UK's Overseas Production Order framework and the EU's European Production and Preservation Orders. Nevertheless, faster acquisition should not come at the expense of forensic documentation or procedural safeguards. Speed improves evidence availability, but does not independently establish evidentiary reliability.

10.13. Service-Provider Jurisdiction and Compliance

Global service providers may simultaneously operate in several jurisdictions and face competing legal obligations concerning disclosure, confidentiality, privacy and data transfer. A provider may receive a legally valid request from one jurisdiction while being subject to restrictions imposed by another. Provider structure can also complicate identifying which legal entity controls the requested information.

The EU e-Evidence framework responds partly to this problem through designated establishments and legal representatives. The UK's Overseas Production Order framework likewise provides a direct mechanism in qualifying international cooperation arrangements. Outside such specialized systems, investigators may remain dependent on MLA, applicable treaties, domestic procedures or other forms of provider cooperation. Provider compliance should therefore be considered both a legal-cooperation issue and a forensic-provenance issue, because the manner in which a provider identifies, extracts and transmits information can affect its subsequent authentication.

10.14. Differences in Procedural and Forensic Standards

The final challenge concerns differences in procedural safeguards and forensic practices. Jurisdictions vary in requirements concerning judicial authorization, notification, proportionality, defence rights, privacy, certification, expert evidence and remedies. They may also differ in forensic quality systems, documentation practices and expectations concerning electronic-evidence authentication.

A forensic method accepted as routine in the acquiring jurisdiction may therefore require further explanation before the receiving court. These differences demonstrate why cross-border evidence interoperability requires more than harmonized access mechanisms. It also requires sufficient documentation to allow the receiving legal system to evaluate how evidence was acquired, preserved,

verified, analysed and transferred. Overall, the principal challenge is not merely obtaining electronic evidence across national boundaries. It is obtaining it lawfully, promptly and in a form whose provenance, authenticity, integrity and reliability remain demonstrable before the receiving court.

Table 4: Major Cross-Border Digital-Evidence Challenges and Their Legal and Forensic

Challenge	Legal / Forensic Implication
Jurisdictional conflicts	Uncertainty over which state may lawfully obtain, compel disclosure of or use evidence.
Data sovereignty and transfer restrictions	Foreign evidence demands may conflict with domestic disclosure or international-transfer rules.
Distributed cloud storage	Data location may be multiple, shifting or unknown, complicating territorial jurisdiction and forensic acquisition.
Remote access	Technical accessibility does not necessarily establish lawful authority to access foreign-controlled data.
Provider-controlled acquisition	Investigators may lack direct control over extraction, requiring stronger provenance and production documentation.
Encryption	Lawfully obtainable evidence may remain technically inaccessible or unreadable.
Metadata, logs and volatile evidence	Delay or incomplete preservation may result in loss of contextual information necessary for reconstruction or authentication.
Different authentication standards	Evidence obtained abroad may require additional proof before the receiving court.
Chain-of-custody gaps	Undocumented transfers or access may weaken integrity, reliability or evidential weight.
Privacy and data protection	Acquisition or international transfer may conflict with privacy and personal-data obligations.
MLA delays	Relevant electronic information may disappear before conventional cooperation procedures are completed.
Service-provider conflicts	Providers may face competing disclosure, privacy and jurisdictional obligations.
Different procedural/forensic standards	Differences in authorization, forensic practices and evidentiary requirements may complicate courtroom use.

11. COMPARATIVE FINDINGS AND DISCUSSION

The comparative analysis reveals substantial convergence in the objectives underlying digital-evidence law, but considerable divergence in the mechanisms used to achieve those objectives. Across the United Kingdom, European Union, Saudi Arabia, India and South Africa, electronic evidence may form part of legal proceedings, while authenticity, integrity, reliability, preservation and procedural legality remain important considerations. The principal differences concern how these concepts are established, how foreign-held evidence is acquired, how service providers participate, and how forensic integrity is demonstrated after cross-border transfer.

The findings support the central proposition of this study: lawful acquisition, forensic integrity and courtroom admissibility are interconnected but distinct stages of the digital-evidence process. A lawful cross-border mechanism establishes authority to obtain evidence. It does not, by itself, establish the authenticity, completeness or reliability of the material ultimately presented before a court.

11.1. Areas of Legal and Forensic Convergence

The strongest area of convergence concerns recognition of the evidentiary importance of authenticity and integrity. Although the five jurisdictions express these concepts through different statutory and procedural frameworks, each requires some basis for determining whether electronic material can reliably be connected to its claimed source.

Preservation is similarly important. Digital evidence can be deleted, overwritten or modified rapidly, making early preservation essential to both investigation and subsequent evidentiary assessment. International mechanisms such as the Budapest Convention framework and the EU's electronic-evidence regime demonstrate the growing importance of expedited preservation in cross-border investigations (Casino et al., 2022).

Forensic practices reinforce these legal objectives. Forensic imaging, appropriate acquisition methods, cryptographic hashing, metadata preservation, log analysis, timestamp interpretation, documentation and chain-of-custody records can provide technical support for authenticity and integrity (Casey, 2011; Turner, 2005; Horsman, 2023).

The convergence is therefore functional rather than uniform. The jurisdictions do not necessarily impose identical technical or statutory requirements, but they confront the same underlying problem: demonstrating that electronic evidence is sufficiently identifiable, preserved and reliable for judicial evaluation.

11.2. Areas of Legal and Procedural Divergence

The principal differences concern how evidentiary reliability is established and how foreign-held evidence is obtained. England and Wales combine general evidentiary principles with a comparatively formalized forensic-quality framework. The statutory Forensic Science Regulator regime provides an additional structure for evaluating forensic processes, although non-compliance does not automatically determine admissibility.

The European Union differs because its major contribution is increasingly focused on cross-border acquisition and preservation. Regulation (EU) 2023/1543 provides European Production and Preservation Orders, while Directive (EU) 2023/1544 establishes institutional arrangements concerning service-provider representation. These mechanisms facilitate access to evidence but do not create a single EU-wide rule governing courtroom admissibility.

Saudi Arabia presents a distinct combination of criminal procedure, cybercrime legislation, electronic-transactions rules, data-protection requirements and statutory provisions concerning digital evidence within their applicable scope. This framework should not be treated as equivalent to either the EU system or a common-law evidentiary model.

India provides comparatively detailed statutory treatment of electronic and digital records under the Bharatiya Sakshya Adhiniyam 2023, including requirements relevant to specified electronic records and accompanying technical information. South Africa's Electronic Communications and Transactions Act adopts a different approach by expressly addressing the admissibility and evidential weight of data messages and identifying factors relating to reliability, integrity and origin. The comparative finding is therefore not that one universal admissibility model exists, but that similar evidentiary objectives are implemented through materially different legal structures.

11.3. Relationship between Forensic Integrity and Admissibility

Forensic integrity provides the technical foundation upon which claims of authenticity and reliability can be evaluated. Hash verification, secure preservation, validated methods, metadata and log analysis, documentation and chain-of-custody records can reduce uncertainty concerning alteration, contamination or misidentification (Casey, 2011; Horsman, 2023). However, technical integrity should not be equated with legal admissibility.

A forensic image may have matching hash values yet still raise questions about whether the original acquisition was legally authorized. Conversely, evidence may have been obtained under valid legal authority while remaining difficult to authenticate because provenance, metadata or handling documentation is incomplete.

The relationship can therefore be expressed as:

Lawful Acquisition → Forensic Integrity → Authentication and Reliability → Judicial
Admissibility

These stages interact, but successful completion of one does not automatically establish the next. This distinction becomes particularly significant in cross-border proceedings because the authority responsible for acquisition may differ from the authority responsible for forensic examination and from the court ultimately assessing the evidence.

11.4. Domestic Admissibility versus Cross-Border Acquisition

One of the principal findings of this study is the distinction between the law governing acquisition and the law governing courtroom use. Cross-border cooperation mechanisms principally address how investigators obtain or preserve evidence beyond their own territorial jurisdiction. They do not necessarily determine whether the resulting material satisfies the evidentiary requirements of the receiving court.

Evidence obtained through MLA, an Overseas Production Order, a European Production Order or another lawful mechanism may therefore still require authentication, provenance evidence, integrity verification and chain-of-custody documentation. The reverse problem is also possible. Digital material may be technically authentic and forensically reliable while raising legal difficulties because the method used to obtain it exceeded applicable authority or failed to comply with required procedural safeguards.

Cross-border investigators should therefore anticipate the receiving jurisdiction's evidentiary requirements before acquisition and transfer, rather than treating admissibility as an issue arising only when the evidence reaches court.

11.5. Effectiveness of International Cooperation Mechanisms

Traditional mutual legal assistance remains important because it provides a formal state-to-state mechanism for obtaining evidence abroad. Its principal weakness in digital investigations is the potential mismatch between procedural timescales and the volatility of electronic information (James & Gladyshev, 2016).

More recent frameworks seek to reduce this problem through expedited preservation and more direct forms of cooperation. The Second Additional Protocol to the Budapest Convention expands mechanisms for electronic-evidence cooperation, while the EU e-Evidence framework provides dedicated production and preservation procedures involving service providers. The United Kingdom's Overseas Production Order framework similarly provides a mechanism for obtaining electronic data from overseas providers where the required international cooperation arrangement applies.

Saudi Arabia, India and South Africa rely on their respective domestic powers together with applicable international cooperation mechanisms for foreign-held evidence. These developments indicate a movement toward faster access, particularly where evidence is held by global providers. However, faster acquisition does not eliminate the need for forensic verification. Evidence obtained rapidly may still encounter problems if provider production, metadata, integrity information or subsequent handling is inadequately documented.

11.6. Cloud Evidence and the Changing Forensic Model

Cloud computing changes the traditional relationship between investigator and evidence. Conventional digital forensics often assumes that investigators can obtain physical media or create a controlled forensic image. Cloud investigations may instead depend on evidence selected, extracted and transmitted by a service provider. This produces a partial shift from examiner-controlled acquisition to provider-mediated acquisition.

The resulting evidentiary questions include whether the production represents the requested dataset, whether relevant metadata and logs were preserved, whether timestamps can be interpreted

reliably, whether the extraction process is documented and whether the received material remained unchanged after production.

Distributed storage further complicates jurisdiction because physical server location may be multiple, dynamic or unknown (Daskal, 2015; Woods, 2016). The relevant legal connection may consequently depend increasingly on provider control, establishment, user location or applicable statutory mechanisms rather than physical storage alone. Cloud evidence therefore demonstrates particularly clearly why lawful access and forensic reliability must be evaluated separately.

11.7. Implications for Investigators, Examiners and Prosecutors

The findings have different implications for participants in the evidentiary process. Investigators should identify jurisdictional issues, preservation requirements, provider control and applicable legal authority as early as possible. Delays can result in the loss of volatile logs, metadata or account information.

Forensic examiners should document acquisition methods, tool versions, hash values, metadata, timestamps, errors, transformations and analytical procedures. Where evidence originates from a provider rather than direct forensic acquisition, examiners should establish precisely what was produced and preserve accompanying provenance information. Prosecutors should evaluate both sides of the evidentiary process: whether the evidence was lawfully obtained and whether a sufficient foundation exists to demonstrate its authenticity and reliability before the receiving court. This coordinated approach reduces the risk that legally obtainable evidence becomes difficult to use because evidentiary requirements were considered too late.

11.8. Implications for Courts

Courts increasingly encounter digital evidence produced through technically and legally complex processes involving foreign authorities, cloud providers and forensic specialists. Judicial assessment should therefore distinguish among several questions: whether acquisition was lawful, whether the evidence has been authenticated, whether its integrity was maintained, whether the forensic methodology was reliable, whether continuity of custody can be demonstrated and what evidential weight should ultimately be attached to the material.

A weakness in one dimension should not automatically be treated as proof of failure in every other dimension. For example, a chain-of-custody issue may raise questions concerning reliability without necessarily establishing that the underlying data were altered. The legal consequence will depend on the governing evidentiary framework and circumstances of the case. This distinction enables courts to evaluate digital evidence more precisely rather than treating technical integrity and legal admissibility as interchangeable concepts.

11.9. Implications across the Five Jurisdictions

The comparison of the United Kingdom, European Union, Saudi Arabia, India and South Africa demonstrates that formal legal recognition of electronic evidence is only one component of effective cross-border evidence practice.

The jurisdictions differ in their mechanisms for authentication, preservation, provider cooperation, international acquisition and judicial evaluation. Their forensic environments also differ in the extent to which technical standards and evidentiary procedures are formally integrated. Saudi Arabia's inclusion particularly broadens the comparison beyond the original common-law and European emphasis. Its combination of criminal-procedure, cybercrime, electronic-transactions and personal-data rules demonstrates how cross-border digital evidence may operate within a substantially different regulatory structure. The broader comparative finding is that interoperability requires coordination between legal authority and forensic practice. Evidence crossing borders should be accompanied by sufficient information about its provenance, acquisition, preservation, integrity and handling to permit meaningful assessment under the receiving jurisdiction's rules.

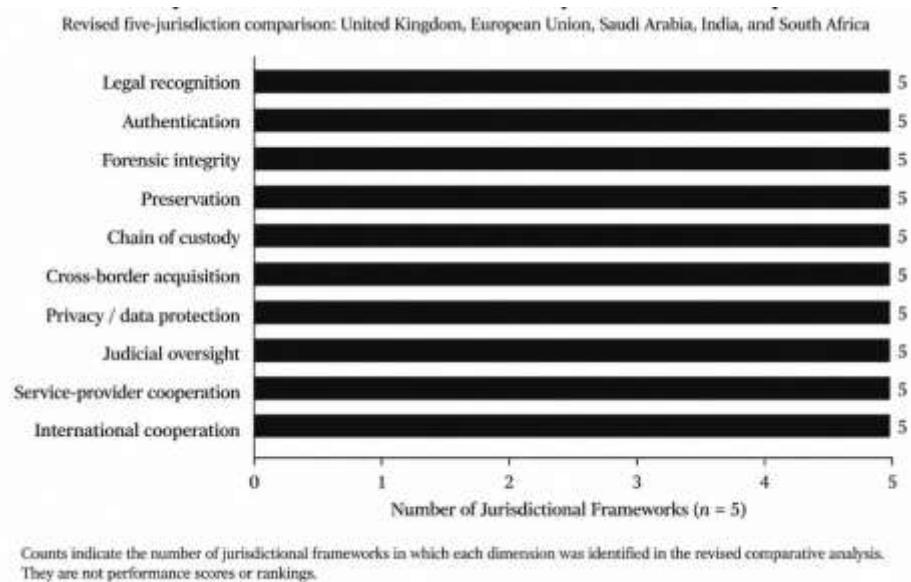


Fig 4 – Comparative Distribution of Core Evidentiary and Procedural Requirements

11.10. Overall Comparative Finding

The study identifies three interconnected requirements for effective cross-border digital evidence:

Lawful Acquisition → Demonstrable Forensic Integrity → Courtroom Admissibility

The first concerns legal authority. The second concerns the technical reliability and continuity of the evidence. The third concerns whether the evidence satisfies the applicable rules of the receiving court. The principal weakness in existing cross-border practice arises where these stages are treated independently. International mechanisms may improve access to foreign-held evidence without

harmonizing evidentiary standards, while technically sophisticated forensic procedures cannot cure every defect in legal authority.

Effective cross-border cybercrime investigation therefore requires greater interoperability between international cooperation mechanisms, domestic procedural law, forensic standards, provider practices and evidentiary requirements. This is particularly important as cloud computing increasingly separates the location of evidence from the location of the persons, providers and authorities controlling it.

12. LEGAL AND POLICY IMPLICATIONS

The comparative findings indicate that improving cross-border digital-evidence practice requires more than faster mechanisms for obtaining data. Reform must connect legal authority with forensic reliability and the evidentiary requirements of the receiving jurisdiction. The existing manuscript already identifies harmonized forensic standards, chain of custody, preservation, judicial oversight, international cooperation and provider accountability as key reform areas. The revised analysis adds greater emphasis on cloud evidence, metadata, provider-mediated acquisition and technical interoperability.

12.1. Toward Harmonized Digital-Forensic Standards

Greater alignment of minimum digital-forensic standards would improve the reliability and portability of evidence across jurisdictions. Harmonization does not require identical national evidence laws. Rather, jurisdictions can establish compatible minimum practices for acquisition, preservation, integrity verification, examination and documentation.

Such standards should address forensic imaging where appropriate, logical and physical acquisition, cloud collection, cryptographic hashing, metadata preservation, log analysis, timestamp interpretation, secure storage and validated forensic methods (Casey, 2011; Horsman, 2023). Standardization is particularly important where evidence obtained in one jurisdiction will be examined or presented in another. The receiving authority should be able to determine what was acquired, how it was acquired, whether it changed and what forensic processes were subsequently applied.

12.2. Standardization of Chain-of-Custody Procedures

Cross-border evidence requires a chain of custody capable of surviving multiple institutional and national transfers. A minimum standardized record should identify the evidence, source, acquisition method, date and time, persons or organizations responsible, integrity checks, transfers, access events, forensic actions and storage conditions.

For provider-held evidence, the record should additionally document the legal request, provider response, production date, account or system concerned, production format and available integrity or provenance information. Standardized documentation would not determine admissibility

automatically, but it would enable courts and forensic examiners in receiving jurisdictions to reconstruct the history of the evidence more reliably.

12.3. Improving Cross-Border Preservation Mechanisms

Rapid preservation remains essential because electronic information may be deleted, overwritten or become inaccessible before formal production procedures are completed. The existing manuscript correctly identifies expedited preservation as a major policy requirement. Preservation mechanisms should cover not only substantive content but also relevant metadata, logs, timestamps, account information and audit records where legally permissible and technically available.

International cooperation should therefore distinguish clearly between preservation and production. Preservation prevents relevant information from disappearing, while production provides the subsequent legal mechanism through which authorities obtain it. Neither process alone establishes admissibility. Preserved and produced evidence must still be appropriately authenticated and subjected to forensic evaluation.

12.4. Strengthening Cloud-Forensics Procedures

Cloud computing requires forensic procedures adapted to evidence that investigators may never physically possess at its original storage location. Where service providers perform the initial extraction, minimum documentation should record the scope of the request, account or system involved, production method, date and time, export format, available metadata, relevant logs and integrity information.

Policies should also distinguish between a forensic image of a physical device and a provider-generated cloud export. These are not technically equivalent forms of acquisition. Cloud-forensics procedures should further address replicated data, changing storage locations, timestamp normalization, retention periods, remote access and encryption. These measures would make it easier for courts to evaluate provenance even where investigators cannot independently reproduce the provider's original extraction process.

12.5. Strengthening Judicial Oversight and Procedural Safeguards

Efficiency in cross-border acquisition should not eliminate appropriate legal oversight. Depending on the applicable framework and investigative measure, authorization procedures should address legality, necessity, proportionality, privacy and available remedies. This becomes particularly important with remote access and provider-directed production because technical capability may allow investigators to obtain information without physically entering another jurisdiction.

Legal frameworks should therefore clearly distinguish technical accessibility from lawful authority. Judicial oversight should also remain separate from forensic assessment. Authorization to obtain evidence answers the question of lawful acquisition, whereas subsequent forensic procedures address authenticity, integrity and reliability.

12.6. Improving International Cooperation

International cooperation mechanisms should combine the legitimacy of formal state-to-state procedures with the speed required for volatile electronic evidence. Traditional MLA remains important, but its effectiveness can be strengthened through clearer competent-authority channels, standardized requests, expedited preservation, secure transmission and defined procedures for resolving conflicts of law (James & Gladyshev, 2016).

More recent mechanisms demonstrate the movement toward faster access and provider cooperation. Nevertheless, their effectiveness should be assessed not only by how quickly evidence is produced but also by whether sufficient provenance and integrity information accompanies that production. The policy objective should therefore be rapid but forensically defensible acquisition.

12.7. Service-Provider Cooperation and Accountability

Service providers increasingly function as evidentiary intermediaries because they control cloud files, communications, subscriber information, access records, authentication logs and other potentially relevant material. Clear procedures are needed for receiving lawful requests, verifying requesting authorities, preserving responsive data, documenting extraction procedures, transmitting evidence securely and protecting affected users' legal rights.

Providers should also preserve sufficient information to explain the provenance of produced material where appropriate. This may include relevant account identifiers, production dates, metadata, export information and integrity values. Such documentation is especially important because investigators may have limited visibility into the provider's underlying infrastructure. Provider cooperation should therefore be understood not simply as a disclosure mechanism but as part of the forensic provenance chain.

12.8. Capacity Building across Jurisdictions

The original manuscript framed this issue specifically as capacity building in “emerging jurisdictions” and referred to India, Nigeria and South Africa. Because Nigeria has been replaced by Saudi Arabia and the revised study uses a broader comparative structure, the heading should instead be Capacity Building Across Jurisdictions. Effective digital-evidence practice requires trained forensic personnel, appropriate laboratories, validated tools, secure evidence-management systems and judicial understanding of digital evidence.

Capacity building should therefore include continuing professional training for investigators, forensic examiners, prosecutors and judges. Particular attention should be given to cloud forensics, provider-generated evidence, metadata and log interpretation, encryption, forensic-tool validation and cross-border chain-of-custody documentation. International training and technical cooperation can also promote more compatible practices without requiring jurisdictions to abandon their distinct evidentiary systems.

12.9. Interoperability of Digital-Forensic Practices

Interoperability is one of the most important implications of the comparative analysis. Evidence crossing borders should remain understandable and technically assessable by authorities operating under different legal systems. Minimum interoperability should address evidence formats, metadata preservation, hashing, timestamps, documentation, secure transmission, tool reporting and chain-of-custody records.

For cloud evidence, interoperability should also address provider export formats and documentation describing how information was identified and extracted. The objective is not complete legal uniformity. Rather, it is to ensure that evidence acquired in one jurisdiction arrives in another with enough technical and procedural information for its provenance, authenticity, integrity and reliability to be meaningfully assessed.

12.10. Integrating Acquisition, Integrity and Admissibility

The principal policy implication of this study is that cross-border digital-evidence reform should not treat acquisition, forensic examination and courtroom admissibility as separate policy domains.

A more integrated model is:

Lawful Acquisition → Preservation → Forensic Integrity → Authentication and Chain of Custody →
Judicial Admissibility

International instruments primarily addressing acquisition should therefore consider the forensic information necessary for subsequent authentication. Domestic forensic procedures should anticipate cross-border transfers. Evidentiary rules should, in turn, permit courts to evaluate how technical and procedural safeguards operated throughout the evidence lifecycle. This integrated approach directly addresses the central problem identified by the study: digital evidence may be lawfully obtained yet remain evidentially vulnerable if authenticity, integrity, provenance or chain of custody cannot subsequently be demonstrated.

13. LIMITATIONS AND FUTURE RESEARCH

13.1. Limitations of the Comparative Legal Approach

This study uses a comparative doctrinal approach to examine digital forensics and evidentiary admissibility across the United Kingdom, European Union, Saudi Arabia, India and South Africa. While this enables comparison of legislation, procedures and international instruments, it cannot fully show how consistently these rules are applied in practice. Operational approaches may differ among investigators, forensic laboratories, prosecutors, courts and service providers.

13.2. Jurisdictional and Legislative Change

Cybercrime, digital-evidence and data-protection laws continue to evolve. The analysis reflects the legal position as of September 2026, and later legislation, case law, treaty developments or

regulatory guidance may affect some conclusions. This is especially relevant to the European Union, where Regulation (EU) 2023/1543 became applicable on 18 August 2026. Its long-term effects on provider compliance, cross-border evidence acquisition and national proceedings remain uncertain.

13.3. Limitations of Available Case Law

Published judgments do not capture every dispute involving electronic evidence, and access to reported decisions varies across jurisdictions. The volume of available case law therefore does not necessarily reflect the actual frequency of digital-evidence disputes. Comparative analysis is also complicated by differences in terminology, particularly concepts such as authentication, integrity, reliability, chain of custody and evidential weight.

13.4. Limitations of the Technical Analysis

The study examines forensic imaging, hashing, metadata, timestamps, logs, encryption, cloud acquisition, tool validation and chain of custody through legal and forensic literature. It does not experimentally test forensic tools or acquisition techniques. Cloud evidence presents an additional limitation because provider-controlled extraction methods and infrastructure are not always publicly accessible or independently verifiable.

13.5. Future Empirical and Technical Research

Future research should test these doctrinal findings through interviews, surveys and case-based studies involving investigators, forensic examiners, prosecutors, judges and service providers. Such research could examine preservation delays, authentication disputes, chain-of-custody failures and the frequency of admissibility challenges involving cross-border digital evidence. Further research should also address cloud and provider-mediated evidence, including metadata, logs, timestamps, export formats, distributed storage, multi-cloud environments and remote acquisition.

13.6. Emerging Technologies and Comparative Research

Encryption, artificial intelligence, deepfakes, Internet of Things devices and automated forensic tools will create new evidentiary challenges. Future studies should examine validation, explainability and reproducibility requirements for AI-assisted forensic analysis.

Comparative research should also assess the practical impact of newer cross-border mechanisms, particularly the EU e-Evidence framework, including whether faster production reduces delays, preserves forensic provenance and limits admissibility disputes. Ultimately, future research should examine not only whether digital evidence can be obtained across borders, but whether it can retain the legal and forensic qualities required for reliable courtroom use.

14. CONCLUSION

Cross-border cybercrime investigations expose a fundamental tension between the global nature of digital evidence and the territorial structure of criminal law. Evidence may be generated in one jurisdiction, stored or replicated in another, controlled by a provider elsewhere, and ultimately

presented before a court operating under different evidentiary rules. This study examined that problem across the United Kingdom, European Union, Saudi Arabia, India and South Africa, focusing on lawful acquisition, authentication, forensic integrity, chain of custody, cloud evidence, service-provider cooperation and admissibility.

The comparison shows that all five frameworks recognize the importance of electronic evidence but differ in how it is acquired, preserved, authenticated and evaluated. International and regional mechanisms can facilitate preservation and production, but they do not remove the evidentiary requirements of the receiving legal system.

The central finding is that lawful acquisition does not automatically establish courtroom admissibility. Legal authority determines whether evidence may properly be obtained, while forensic processes help demonstrate its provenance, integrity and reliability. Appropriate acquisition, hashing, metadata and log preservation, timestamp analysis, validated methods, documentation and continuous chain-of-custody records therefore remain essential, particularly for cloud and provider-mediated evidence where investigators may have limited control over the original extraction.

The relationship can be summarized as:

Lawful Acquisition → Forensic Integrity → Courtroom Admissibility

Weakness at any stage can affect the next. Lawfully obtained evidence may remain difficult to authenticate, while technically reliable evidence may face legal difficulties if its acquisition violated applicable procedural requirements.

Effective reform therefore requires greater interoperability between international cooperation mechanisms, domestic procedural law, digital-forensic standards, service-provider practices, data-protection safeguards and evidentiary requirements. Standardized documentation, rapid preservation, reliable integrity verification, transparent provider production and defensible chains of custody can strengthen judicial assessment.

Ultimately, cross-border digital-evidence cooperation should not be measured only by whether investigators can obtain data. The critical issue is whether evidence can move across jurisdictions and through forensic examination while retaining the legal and technical foundations necessary for reliable courtroom use.

REFERENCE

- [1] Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, 8(1), tyac014.
- [2] James, J. I., & Gladyshev, P. (2016). A survey of mutual legal assistance involving digital evidence. *Digital Investigation*, 18, 23–32. doi:10.1016/j.diin.2016.06.004.
- [3] Blažič, B. J., & Klobučar, T. (2020). Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society. *Information & Communications Technology Law*, 29(1), 66–81.

- [4] Zhang, H., & Gong, X. (2024). The research on an electronic evidence forensic system for cross-border cybercrime. *The International Journal of Evidence & Proof*, 28(1), 21-44.
- [5] Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation. *New Journal of European Criminal Law*, 15(3), 256-274.
- [6] Shurson, J. (2025). The balance of efficiency and fundamental rights in the EU e-Evidence Regulation. *New Journal of European Criminal Law*, 16(3), 278-299.
- [7] Daskal, J. (2015). The un-territoriality of data. *Yale IJ*, 125, 326.
- [8] Woods, A. K. (2016). Against data exceptionalism. *Stan. L. Rev.*, 68, 729.
- [9] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
- [10] Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & justice*, 63(1), 116-126.
- [11] Potla, R. (2023). Designing a BTP-centric integration mesh for shop-floor IoT, MES and ERP in discrete manufacturing. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 1(2), 1-8.
- [12] Burri, X., Casey, E., Bolle, T., & Jaquet-Chiffelle, D. O. (2020). Chronological independently verifiable electronic chain of custody ledger using blockchain technology. *Forensic Science International: Digital Investigation*, 33, 300976.
- [13] Adelusi, A. J. (2026). Evaluating AI-Driven Cybersecurity Systems: Effectiveness, Adversarial Risks, and Ethical Considerations. *International Journal of AI, BigData, Computational and Management Studies*, 7(1), 274-285. <https://doi.org/10.63282/3050-9416.IJAIBDCMS-V7I1P142>
- [14] Turner, P. (2005). Unification of digital evidence from disparate sources (digital evidence bags). *Digital Investigation*, 2(3), 223-228.
- [15] Turner, P. (2007). Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags. *Digital Investigation*, 4(1), 30-35.
- [16] Kyei, K., Zavorsky, P., Lindskog, D., & Ruhl, R. (2012, October). A review and comparative study of digital forensic investigation models. In *International conference on digital forensics and cyber crime* (pp. 314-327). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [17] Ismail, I., & Akram Zainol Ariffin, K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS One*, 20(9), e0331683.
- [18] Chadha, V., & Sivaraman, J. (2024). Critical analysis of the law on admissibility of electronic evidence in India. *Jindal Global Law Review*, 15(1), 119-132.
- [19] Roberts, P., & Zuckerman, A. (2022). *Roberts & Zuckerman's criminal evidence*. Oxford University Press.
- [20] Swales, L. (2018). An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform-Part Two. *Potchefstroom Electronic Law Journal (PELJ)*, 21(1), 1-34.
- [21] Potla, R. B. (2022). ISCSITR–International Journal of ERP and CRM (ISCSITR. *IJEC*, 3(1), 11-38.
- [22] Roux, C., Crispino, F., & Ribaux, O. (2012). From forensics to forensic science. *Current Issues in Criminal Justice*, 24(1), 7-24.
- [23] Marcén, A. G. (2024). The Budapest convention and the UN cybercrime convention negotiations. In *Global cybersecurity and international law* (pp. 174-192). Routledge.
- [24] Rica, C., & Macedonia, N. (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence.
- [25] Belfiore, R. (2015). The European Investigation Order in criminal matters: developments in evidence-gathering across the EU. *Eur. Crim. L. Rev.*, 5, 312.
- [26] Regulation, G. D. P. (2016). European Parliament, Council of the European Union. Regulation, 679.
- [27] Beqiraj, P., Gjipali, D., & Jançe, K. (2024). The Integral Role of the Albanian Parliament in EU Integration through National Law Approximation (January 2018-December 2023). *Access to Just. E. Eur.*, 169.
- [28] United Kingdom. (1984). *Police and Criminal Evidence Act 1984*, c. 60.
- [29] Olley, N. (2019). 207 Transnational policing and organised crime. *The Development of Transnational Policing: Past, Present and Future*, 207-238.
- [30] Adelusi, A. J. (2026). Enhancing Cybersecurity Resilience in U.S. Financial Infrastructure: A Risk-Based and Regulatory Approach. *International Journal of Artificial Intelligence and Engineering Research*, 2(01). <https://research-education.com/index.php/ijaie/article/view/38>

-
- [31] Benhafsi, S. (2025). " Digital Forensics is the Newest, Most Troublesome Forensic Discipline": A Critical Examination of the Use of Digital Forensics in the Investigation and Prosecution of Major Crime in England and Wales (Doctoral dissertation, University of South Wales (United Kingdom)).
- [32] El Said, M. (2018). Intellectual property law in Saudi Arabia. Kluwer Law International BV.
- [33] Said, M. E. (2018). Intellectual Property Law in Saudi Arabia.
- [34] Waksmańska, M. (2021). The procedural principles in criminal proceedings in the Kingdom of Saudi Arabia and the Arab Republic of Egypt. In *Oriental Meetings in Sosnowiec Language, Literature, Society Sosnowieckie Spotkania Orientalistyczne* Język, literatura, społeczeństwo (p. 145).
- [35] Alangari, A. (2021). A Proposal for Omnibus Legal Reform of Saudi Construction Practices to Meet Economic Development Goals in Saudi Arabia: An Initiative for Legislative Reform Towards Effective and Codified Judicial Remedies, Compatible with Sharia Law and Aligned with Saudi Arabia's Vision 2030. American University.
- [36] Potla, R. B. (2024). A SOX/ITAR-aligned global ERP template for multi-plant manufacturers: Governance patterns and controls. *J Artif Intell Mach Learn & Data Sci*, 2(2), 3222-3232.
- [37] Bamashmoos, A. M. Consent Requirements and Limitations in Saudi Arabia's Personal Data Protection Law: An In-depth Analysis.
- [38] Data, S., & Authority, A. I. (2024). Regulation on Personal Data Transfer Outside the Kingdom. Riyadh: SDAIA.
- [39] Tomar, A. S. The Indian Journal for Research in Law and Management.
- [40] Coetzee, J. (2004). The Electronic Communications and Transactions Act 25 of 2002: facilitating electronic commerce. *Stellenbosch Law Review*, 15(3), 501-521.