 ***DOI:** https://doi.org/10.63108/IJLMH.13188*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

The Legal Framework Governing Digital Evidence in Criminal Proceedings: A Comparative Analytical Study

AADEL ABDULLA ALI ALYAMMAHI*

ABSTRACT

The increasing reliance on digital technologies in the commission and investigation of crime has made digital evidence integral to contemporary criminal proceedings, while raising complex questions concerning its admissibility, reliability, and compatibility with fair-trial guarantees. This study examines the adequacy of the legal regulation of digital evidence in criminal proceedings and the extent to which it reconciles effective criminal investigation with the protection of fundamental rights. Employing descriptive-analytical, comparative, and inductive approaches, it analyses the legal nature of digital evidence, the procedures governing its collection, seizure, preservation, and examination, and the principles guiding its judicial assessment. The study considers selected Arab and international legal frameworks, with particular attention to the United Arab Emirates, and addresses the challenges of obtaining electronic data across national borders. The findings indicate that contemporary legal systems increasingly recognise digital evidence as a legitimate means of criminal proof. The principal challenge lies not in recognition alone, but in safeguarding the legality, integrity, and verifiability of such evidence throughout its lifecycle. A documented chain of custody and competent forensic examination are central to establishing reliability, while the ultimate assessment of probative value remains within the discretion of the criminal court. The study therefore recommends clearer procedural rules specifically tailored to digital evidence, standardised custody and preservation practices, professional standards for forensic expertise, and stronger mechanisms for international judicial cooperation. It concludes that an effective legal framework must integrate technical safeguards with procedural protections to strengthen criminal justice without undermining privacy, defence rights, or the fairness of proceedings.

Keywords: *Digital Evidence, Criminal Proceedings, Admissibility of Evidence, Chain of Custody, Digital Forensics, Comparative Criminal Procedure*

* Author is a Faculty Member at the Police College, Abu Dhabi, United Arab Emirates. ORCID: https://orcid.org/0009-0001-6720-904X

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

I. INTRODUCTION

Electronic communications, cloud storage, mobile devices, and networked services now routinely create information capable of illuminating criminal conduct. A criminal investigation may depend upon messages exchanged through an application, server logs recording remote access, photographs containing location metadata, or a forensic image of a seized device. These materials can establish a sequence of events, corroborate testimony, and sometimes exculpate an accused person. Their evidential significance is not confined to offences conventionally described as cybercrimes: electronically stored information may be relevant to corruption, fraud, violence, financial crime, and almost any other category of criminal conduct.[1]

Digital evidence nevertheless raises distinctive difficulties. Unlike an ordinary physical exhibit, a digital file may be copied without obvious degradation, altered without a visible trace, distributed among several jurisdictions, or rendered unintelligible without specialist tools. Investigators therefore face two related obligations: to obtain the information through lawful procedures and to demonstrate that what is ultimately presented to the court reliably reflects the relevant source. Courts must in turn decide whether the evidence is legally admissible, technically authentic, and persuasive in the context of the entire case. These decisions have consequences for privacy, equality of arms, and the ability of an accused person to challenge the prosecution's technical account.[2]

The central question examined in this study is whether contemporary legal frameworks adequately reconcile the effectiveness of digital criminal evidence with the guarantees of a fair trial. The inquiry is divided into four issues: the legal character and distinctive attributes of digital evidence; the rules governing its identification, collection, seizure, and preservation; the judicial determination of authenticity, admissibility, and probative weight; and the adequacy of international cooperation when the relevant data are controlled or stored abroad. Particular emphasis is placed on the United Arab Emirates (UAE), assessed alongside selected comparative examples.

---

[1] COUNCIL OF EUROPE, Convention on Cybercrime, ETS No. 185, art. 14 (Nov. 23, 2001), https://www.coe.int/en/web/cybercrime/the-budapest-convention; COUNCIL OF EUROPE CYBERCRIME CONVENTION COMMITTEE, *Guidance Note #13: Scope of Procedural Powers and of International Co-operation Provisions of the Budapest Convention*, T-CY(2023)6 (June 2023), https://www.coe.int/en/web/cybercrime/-/t-cy-confirms-broad-scope-of-powers-for-the-collection-of-electronic-evidence-and-international-cooperation%C2%A0; *see also* EUROJUST, *Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence* 3 (SIRIUS Project, Jan. 23, 2024), https://www.eurojust.europa.eu/sites/default/files/assets/the-budapest-convention-on-cybercrime-and-cross-border-access-to-electronic-evidence-23-01-2024.pdf.

[2] SEAN E. GOODISON, ROBERT C. DAVIS & BRIAN A. JACKSON, DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM 1–5, 7, 12–13 (RAND Corp. 2015), https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR890/RAND_RR890.pdf.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The paper is doctrinal; it does not claim to report original interviews, statistical data, or an empirical review of court files. The focus is digital evidence in criminal investigation and adjudication. Civil-law provisions are discussed only to illuminate the broader regulatory environment, not as if they automatically determined the admissibility of criminal proof. The comparative discussion is deliberately selective: Europe, the United States, and certain Arab systems are examined as distinct regulatory examples rather than as a comprehensive survey of every national law. The contribution lies in articulating a connected framework of lawful acquisition, demonstrable integrity, and effective adversarial scrutiny. The proposition advanced is that none of these elements, considered in isolation, is sufficient to secure reliable and rights-compliant use of digital evidence.

The literature approaches electronic evidence from several directions. Kerr examines how rules designed for physical evidence and eyewitness testimony apply to the collection of digital evidence, and Carrier addresses the techniques required to examine file systems.[3] Comparative scholarship, notably Damaška's work on free proof, considers how far the law leaves the weighing of evidence to the fact-finder;[4] technical publications such as the National Institute of Standards and Technology's guide describe forensic practices that support the integrity and reproducibility of results;[5] and institutional research addresses the resources and capacities needed across the criminal justice system. The RAND Corporation's study of digital evidence, for example, underlines both the increasing investigatory importance of digital material and the operational difficulties facing police, prosecutors, and courts.[6]

A persistent problem is that legal analysis and forensic practice are often presented in separate compartments. Rules on search powers may be discussed without specifying how the integrity of seized data should be recorded; conversely, technical discussions may assume that a successful extraction is legally sufficient to justify reliance on the product. This article addresses that disconnect. It treats the evidential process as a continuous sequence, from lawful access to meaningful judicial scrutiny, while maintaining the crucial distinction between technical reliability and legal admissibility. International standards are examined as possible guides for reform, not as automatically binding law in the UAE.

---

[3] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005); BRIAN CARRIER, FILE SYSTEM FORENSIC ANALYSIS (2005).
[4] Mirjan Damaška, *Free Proof and Its Detractors*, 43 AM. J. COMP. L. 343 (1995).
[5] Karen Kent et al., *Guide to Integrating Forensic Techniques into Incident Response* 3-1 to 3-8, 4-7, NIST Spec. Pub. 800-86 (2006), https://doi.org/10.6028/NIST.SP.800-86.
[6] Goodison et al., *supra* note 2, at 1–5, 18.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

II. Concept and Legal Character of Digital Evidence

A. Definition and evidential forms

For the purposes of criminal proceedings, digital evidence may be defined as information generated, stored, transmitted, processed, or recovered through electronic systems that is capable of proving or disproving a fact material to a criminal investigation or trial. Its legal significance derives not from an item's electronic form alone, but from its relevance, the lawfulness of its acquisition, and the reliability of the processes used to identify, preserve, and interpret it. This functional definition includes information recovered from computers, smartphones, storage media, communication networks, application databases, surveillance systems, and cloud services.

Digital evidence takes many forms. It may consist of the content of an electronic message, its sending and receipt times, network connection records, metadata embedded in a photograph, a record produced automatically by an information system, or data recovered from a deleted file. Investigators should distinguish the content of a communication from the surrounding metadata and from subscriber or traffic records, because these categories can trigger different legal powers and privacy interests. Moreover, a record's origin does not necessarily establish who performed the action it appears to represent. The presence of a file on a device, for instance, requires careful assessment before it can be attributed to a particular individual.

The UAE Law of Evidence in Civil and Commercial Transactions offers a broad statutory illustration of electronic evidence: Article 53 defines it in terms of data or information generated, stored, extracted, copied, transmitted, reported, or received through information technology and retrievable in an intelligible form. Article 54 lists electronic records, instruments, signatures, seals, correspondence, modern communication methods, electronic media, and other electronic evidence.[7] These provisions indicate legislative recognition of diverse digital records. Their statutory field, however, is civil and commercial transactions; their classification of electronic evidence cannot simply be treated as a self-executing rule governing criminal prosecutions. Criminal legality and the rules of criminal procedure must be independently examined.

B. Digital evidence and conventional physical exhibits

Electronic information differs from conventional exhibits in several important respects. First, it is generally represented through data structures and requires a technological interface for

[7] Federal Decree-Law No. 35 of 2022, Promulgating the Law of Evidence in Civil and Commercial Transactions, arts. 53–54 (U.A.E.), https://www.uaelegislation.gov.ae/en/legislations/1612/download.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

intelligible interpretation. Second, copies may be produced without changing the underlying bit sequence, provided appropriate acquisition methods are used. Third, data can be overwritten, synchronised, deleted, encrypted, or modified by routine system activity. Fourth, the relevant information may exist simultaneously on a local device, a service provider's server, and several remote backups. Finally, a digital record may combine highly relevant information with extensive unrelated personal material.

These characteristics demand procedural sensitivity. In an ordinary seizure, investigators may describe the physical location, condition, and packaging of an exhibit. In a digital examination they must also be able to identify the acquisition method, original source, time settings, relevant software and tools, forensic image, and measures used to guard against alteration. Cryptographic hash functions can assist by detecting whether two datasets are identical at the time of comparison, but matching hash values cannot independently prove that the original data were lawfully acquired, correctly attributed, or free from manipulation before acquisition.[8]

The claim that digital evidence is invariably objective or scientifically conclusive is therefore misplaced. Every stage contains potential interpretive choices: what device was examined, which user profile was selected, what deleted data could be recovered, how timestamps were normalised, and how conflicting records were understood. A technically accurate extraction can still support an incorrect inference concerning authorship, intention, or the chronology of events. Forensic correctness and judicial proof overlap, but they are not identical.

C. Legal admissibility, authenticity, and probative value

Three concepts should be kept distinct. Admissibility concerns whether the law permits the court to receive and consider an item. Authenticity concerns whether the item is what the presenting party claims it to be. Probative value concerns the strength of the inference that the item reasonably supports when considered with other evidence. A digital file can be authentic yet legally inadmissible if collected through an unlawful procedure; it may be lawfully obtained but of limited weight if its connection to the accused is uncertain. The converse is also true: technically complex evidence does not necessarily deserve greater weight merely because it was generated by a computer.

A persuasive evidential framework must therefore address the legal basis for acquiring the record, the credibility of its technical provenance, and the opportunity for forensic findings to be tested. The present analysis emphasises that digital evidence remains subject to judicial

[8] Fed. R. Evid. 902(14) advisory committee's note to 2017 amendment, https://www.law.cornell.edu/rules/fre/rule_902; Kent et al., *supra* note 5, at 3-1 to 3-8.

evaluation rather than enjoying a predetermined superior evidential status. This approach prevents the court from delegating its constitutional and procedural responsibility to the expert who produced a forensic report.

III. COMPARATIVE LEGAL REGULATION

A. International model: the Budapest Convention

The Council of Europe's Convention on Cybercrime (2001), commonly known as the Budapest Convention, supplies a prominent comparative reference point for the investigation of cybercrime and the securing of electronic evidence. Its procedural architecture addresses expedited preservation of stored computer data, preservation and partial disclosure of traffic data, production orders, and search and seizure of stored computer data. These powers operate alongside provisions on safeguards and international cooperation.[9] A distinction should be drawn between preserving data so that it is not lost and obtaining substantive access to that data; the latter can require a further legal basis and additional safeguards.

The Convention also illustrates why purely domestic rules are inadequate when data are transient and transnational. Service providers may be established in one jurisdiction while information is stored, processed, or accessed in another. Investigators need mechanisms capable of acting promptly without circumventing the legal protections of either jurisdiction. The Second Additional Protocol, opened for signature in 2022, further develops mechanisms for international cooperation and disclosure of electronic evidence. According to the Council of Europe's treaty-status record as of September 2026, the Second Additional Protocol had not yet entered into force.[10] The Convention and Protocol are considered as comparative models: their discussion does not imply that every state examined is a party or bound by every instrument.

Two principles are particularly important. First, procedural authorities should be capable of securing at-risk data before it disappears. Second, the ability to act quickly should be matched by an identifiable legal threshold, appropriate supervision, limited scope, and remedies for improper intrusion. International cooperation should not dilute safeguards simply because the evidence is accessible through a foreign company or remotely located server.

---

[9] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, arts. 15–19, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[10] COUNCIL OF EUROPE, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, C.E.T.S. No. 224 (2022), https://www.coe.int/en/web/cybercrime/the-budapest-convention. *See also* COUNCIL OF EUROPE TREATY OFFICE, Chart of Signatures and Ratifications, CETS No. 224 (status Sept. 12, 2026), https://www.coe.int/en/web/conventions/full-list/?module=signatures-by-treaty&treatynum=224.

B. European and French developments

European systems demonstrate efforts to reconcile evidence-gathering powers with privacy and procedural fairness. In England and Wales, the framework relies upon general criminal procedure: the Police and Criminal Evidence Act 1984 extends powers of seizure to information stored in electronic form and allows a court to refuse prosecution evidence whose admission would have such an adverse effect on the fairness of the proceedings that it ought not to be admitted.[11] That framework is supplemented by the Forensic Science Regulator's statutory Code of Practice, which requires chain-of-custody records and contains a dedicated section on digital forensics.[12] France provides a clear articulation of judicial assessment: Article 427 of the French Code of Criminal Procedure, in force during 2026, generally permits offences to be proved by any means of evidence unless the law provides otherwise, and requires the decision to rely upon evidence presented and debated before the court.[13] This supports the principle that technological evidence must remain open to adversarial challenge.

At the European Union level, Regulation (EU) 2023/1543 creates a framework for European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings. The regulation applies from 18 August 2026 and provides a contemporary example of a structured response to cross-border demands for electronic data.[14] Its distinct production and preservation mechanisms confirm that urgent data security and compulsory disclosure are related but analytically separate functions. The framework also includes procedural conditions and avenues of legal remedy. It would be inaccurate, however, to portray this EU regime as a directly applicable law governing a non-EU jurisdiction such as the UAE.

The comparative implication is not that a single European model should be copied wholesale. It is that legislation can explicitly identify the type of data sought, the authority empowered to act, the legal threshold applicable to that category, the safeguards available to affected persons, and the method through which material obtained abroad may be scrutinised domestically.

---

[11] Police and Criminal Evidence Act 1984, c. 60, §§ 20, 78 (Eng. & Wales), https://www.legislation.gov.uk/ukpga/1984/60/section/20; https://www.legislation.gov.uk/ukpga/1984/60/section/78.

[12] FORENSIC SCIENCE REGULATOR, *Code of Practice: Version 2* §§ 29.2.8, 97 (May 2025), https://assets.publishing.service.gov.uk/media/68401f4be550203c8209cce9/2025_05_20_Code_of_Practice_final.pdf.

[13] CODE DE PROCÉDURE PÉNALE [C. pr. pén.] art. 427 (Fr.), https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037108959/2026-01-15.

[14] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings, arts. 1, 18, 34, 2023 O.J. (L 191) 118, https://eur-lex.europa.eu/eli/reg/2023/1543/oj.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

C. United States: authentication and forensic certification

The United States illustrates an approach in which evidence law has developed specific methods of authenticating electronic records. Federal Rule of Evidence 901 requires a proponent to present sufficient evidence to support a finding that an item is what the proponent claims. Rule 901(b)(9), for example, recognises evidence describing a process or system and showing that it produces accurate results. Rules 902(13) and 902(14) allow specified records generated by electronic processes, and data copied from electronic devices or media, to be authenticated through appropriate certification without always requiring a live witness solely for that foundation.[15]

These rules provide a useful distinction between technical authentication and ultimate admissibility. Even if a copy of data is adequately authenticated through digital identification, the opposing party may contest relevance, hearsay, attribution, or other legal objections. Certification is not a blanket guarantee that every conclusion drawn from an electronic record is correct. The federal framework therefore helps demonstrate how technical evidence can be made accessible to the court without foreclosing meaningful adversarial testing.

A further lesson comes from the institutional demands of digital investigation. Goodison, Davis, and Jackson identify challenges in acquiring, using, and understanding digital information across the criminal justice process, showing that effective proof depends on professional training and organisational capacity as well as evidential rules.[16] Reform must accordingly address the competence of investigators and expert witnesses, access to appropriate technology, and the court's ability to assess apparently authoritative forensic conclusions.

D. Egypt and the wider Arab context

Egyptian legislation offers an explicit example of statutory recognition of digital proof. Article 11 of Law No. 175 of 2018 on combating information technology crimes provides for electronic evidence extracted from devices, media, information systems, programs, or other information technology to possess evidential value comparable to material criminal evidence when the technical conditions prescribed in the law's executive regulations are satisfied.[17] The provision links legal recognition to technical compliance and reveals the legislator's concern with reliable acquisition and examination. The precise content of technical requirements remains important:

[15] Fed. R. Evid. 901(a), 901(b)(9), 902(13)–(14), https://www.law.cornell.edu/rules/fre/rule_901; https://www.law.cornell.edu/rules/fre/rule_902.
[16] Goodison et al., *supra* note 2, at 1–5, 18.
[17] Law No. 175 of 2018 on Combating Information Technology Crimes, art. 11 (Egypt), https://lawhub.info/eg/?p=11428 (Arabic text).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

a general declaration of evidential equality does not remove the need to examine methodology and legality in an individual case.

The decisive challenge, in Egypt as in the UAE examined below, is not simply whether electronic records are acknowledged, but whether authorities, laboratories, prosecutors, and judges operate under transparent and sufficiently precise procedures capable of meeting legal scrutiny.

The region's legal traditions and institutions are not uniform. A productive comparative method therefore avoids broad claims that all Arab systems have adopted identical rules. What can reasonably be drawn from the materials examined is a shared practical need: to convert general acceptance of digital evidence into verifiable rules governing its lifecycle and the protection of affected persons.

IV. The United Arab Emirates: powers, evidence, and safeguards

A. The Criminal Procedures Law as the principal procedural source

In the UAE, Federal Decree-Law No. 38 of 2022, promulgating the Criminal Procedures Law, provides the relevant framework for criminal investigation and trial. Its provisions must be read alongside other applicable criminal and constitutional guarantees rather than displaced by the separate statute governing civil and commercial evidence.[18] The distinction matters because criminal investigators exercise coercive powers and because an accused person faces consequences that demand careful procedural protections.

Article 73(1) of the Criminal Procedures Law permits the prosecutor, where required by the investigation, to search devices, networks, equipment, media, electronic supports, information systems, computer programs, or other technical means, and to engage specialists or experts for that purpose. Article 73(2) permits the monitoring and recording of conversations, including wired and wireless communications, subject to the Attorney General's prior approval.[19] The provision is significant because it expressly recognises technologically mediated searches rather than leaving investigators to rely solely on analogies with physical premises or paper documents.

The distinction between searching stored data and monitoring communications should remain visible in investigative practice. A lawful search of a seized device does not automatically justify indiscriminate interception of communications or access to unrelated accounts. The statutory

[18] Federal Decree-Law No. 38 of 2022, Promulgating the Criminal Procedures Law (U.A.E.), https://www.uaelegislation.gov.ae/en/legislations/1609/download.
[19] *Id.* art. 73(1)–(2).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

reference to prior approval for monitoring underscores the need to assess the legal basis for each intrusive measure. The scope of an authorisation, its implementation, the categories of information acquired, and the treatment of unrelated material are all relevant to subsequent judicial evaluation.

B. Privacy and defence-related protections

Digital devices frequently contain extensive records of private life, including correspondence with relatives, financial information, medical details, and messages relating to professional advice. Investigators seeking one category of records can easily encounter unrelated sensitive data. Legality therefore requires attention to necessity and proportionality in the application of authorised powers, together with traceable decisions on selection, extraction, disclosure, and retention. A technically convenient full-device extraction may generate broader privacy consequences than the investigative question initially demands.

UAE law also recognises protections directly relevant to defence rights. Article 75 of the Criminal Procedures Law restricts seizure of documents delivered by an accused person to counsel for the purpose of legal representation and the review of correspondence between them concerning the case.[20] The legal and forensic teams must accordingly be capable of identifying and separating potentially protected material. The practical challenge is not resolved by simply declaring that software conducted the search. Technological capacity must be accompanied by procedures through which rights-bearing categories of information are respected.

For a court assessing digital proof, the pertinent question extends beyond whether an electronic record exists. It includes whether the collecting authority acted within its powers; whether the method used exceeded the authorised scope; and whether the accused has had a realistic opportunity to understand and contest the origin and interpretation of the evidence. Where foreign providers, encrypted devices, or extensive cloud accounts are involved, these issues can become especially difficult.

C. The Evidence Law: an important but limited comparison

Federal Decree-Law No. 35 of 2022, promulgating the Law of Evidence in Civil and Commercial Transactions, recognises electronic evidence and establishes rules concerning electronic evidential procedures. Article 10 addresses evidentiary procedures undertaken through electronic means; Article 53 defines electronic evidence; and Article 54 enumerates several categories of such evidence.[21] These provisions reflect the UAE's broader movement

[20] *Id.* art. 75.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

toward digital processes in litigation and show that electronic form is not viewed as inherently incompatible with proof.

Nevertheless, the statute's title and subject matter impose a doctrinal boundary. The legal treatment of an electronic instrument in a commercial dispute is not the same question as whether a digitally extracted communication is admissible in a criminal prosecution following an intrusive search. It follows that one should not use the provisions of the civil and commercial Evidence Law as a substitute for the procedural safeguards required under criminal law. The broader legislative recognition is relevant context; the legal authorisation and reliability of criminal digital evidence must be established through the applicable criminal framework.

D. Normative assessment of the UAE framework

The express recognition of digital searches in Article 73 represents a meaningful legal foundation. Yet the existence of a statutory power does not by itself produce a complete forensic protocol for every kind of device, source, or cloud platform. Rules are also needed to translate the authorisation into defensible investigative practice: identifying who acquired the data, how the source was isolated, whether the contents were changed, which tools were used, and how the material was secured after collection.

The need for further specificity should not be understood as a claim that all current UAE investigative practice is deficient. This doctrinal study does not present an empirical audit of police laboratories or criminal court files. Rather, it identifies procedural questions that any digital-evidence regime must answer if courts are to evaluate authenticity, rights compliance, and the reliability of expert conclusions. Regulatory refinement could clarify minimum documentation practices, quality-assurance requirements, rules for privileged information, and the arrangements through which the defence can challenge a technical report.

V. Collection, Preservation, and Forensic Integrity

A. From lawful access to technical acquisition

Digital-evidence collection should begin by establishing the legal basis, evidential purpose, and appropriate scope of the proposed operation. The investigator must identify the devices, accounts, networks, or remote systems likely to contain relevant information and choose procedures that minimise avoidable alteration or loss. Unlike a conventional paper document, a live information system may continue writing data during seizure or examination. As a result,

[21] Federal Decree-Law No. 35 of 2022, Promulgating the Law of Evidence in Civil and Commercial Transactions, arts. 10, 53–54 (U.A.E.), https://www.uaelegislation.gov.ae/en/legislations/1612/download.

the handling strategy must account for transient information, encryption, remote access, and the possibility of automated deletion or synchronisation.

Relevant technical sources include network protocols, Internet Protocol addresses, browser cookies, proxy information, and intrusion-detection or tracing records. These sources can help reconstruct actions and the movement of communications. Nevertheless, none is infallible proof of a particular user's physical location or identity. IP addresses may be shared, reassigned, translated, or routed through intermediaries; cookies may be deleted or duplicated; and logs can have incomplete or inconsistent clocks. Each artefact must be interpreted in the context of the system that generated it and independently corroborated where possible.

A sound acquisition record therefore documents the origin of the data, the authority under which it was obtained, the relevant date and time, the tools and procedures used, and any limitations encountered. The record must also disclose whether the process produced a complete forensic image, a logical extraction, or a narrower export of selected records. These methods can yield different results, and their differences should not be concealed when the evidence is later presented to the court.

B. Chain of custody and integrity verification

The chain of custody is the documented history of an item from collection through preservation, transfer, examination, and presentation. In digital investigations, its purpose is to permit an independent assessment of who handled the material, what occurred during each intervention, and whether the offered record can be reliably linked to the acquired source. A robust chain records responsible persons, transfers, dates and times, storage locations, identifiers, actions performed, and any departure from standard procedures.

Technical safeguards reinforce the documentary record. Investigators may work from forensic copies rather than unnecessarily altering a source device, calculate and compare cryptographic hashes, control access to evidence storage, and retain logs of analytical operations. These practices do not guarantee that the underlying evidence is true, but they can support the narrower and essential proposition that the data have remained sufficiently stable for examination. The National Institute of Standards and Technology's *Guide to Integrating Forensic Techniques into Incident Response* provides an influential technical description of the collection, examination, analysis, and reporting phases of the forensic process, including the identification of data and the preservation of its integrity, while expressly cautioning that its information-technology focus is not a substitute for jurisdiction-specific legal requirements.[22]

[22] Kent et al., *supra* note 5, at ES-1, 1-1, 2-1 to 3-8.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

A break in documentation should not be treated mechanically as creating identical legal consequences in every case. Its significance depends on applicable procedural rules, the nature of the gap, the possibility of alteration, and whether independent evidence can establish continuity. The legal objective is reliable proof supported by transparent procedures, not the unthinking application of a checklist. Nevertheless, systematically missing records of access or extraction will make it much harder for a court to assess whether an exhibit is the same data that were originally secured.

C. Expert examination, disclosure, and reproducibility

Digital forensic experts can explain the operation of an information system, recover information that is not immediately visible, determine whether an extraction method was suitable, and interpret technical artefacts. Their role is indispensable in complex cases, but it is not equivalent to deciding the legal meaning of the evidence. An expert who finds a message or a device identifier cannot automatically establish who authored it, whether that person possessed the required criminal intent, or whether the state lawfully obtained it.

A meaningful expert report should identify the questions asked, materials received, tools and versions used, procedures performed, assumptions made, results obtained, and limitations or alternative interpretations. Where practicable, sufficiently detailed documentation should permit another qualified examiner to reproduce or critically evaluate the findings. Disclosure to the parties should be adequate to allow informed questions about methodology, possible contamination, missing records, and conclusions that exceed what the data support.

Judicial reliance upon expertise consequently demands critical distance. The judge must remain able to distinguish between an expert's observation, a scientific inference, and a conclusion that belongs to the court. The adversarial testing of a technical report is not an obstacle to efficient criminal justice; it is one of the ways in which technically sophisticated evidence becomes legally accountable.

VI. Judicial assessment, fair trial, and transnational access

A. Judicial conviction and the assessment of evidential weight

This study places particular importance on the principle of the criminal judge's assessment of evidence. Within the bounds established by national law, the judge evaluates whether the prosecution's materials are sufficiently persuasive and whether the evidence has been obtained and presented in a legally acceptable manner. The probative effect of a digital artefact cannot be determined from its format alone. An apparently precise timestamp may depend on a

misconfigured device clock; a deleted file may be attributable to automated caching rather than deliberate human activity; and an account credential may have been used by someone other than its nominal owner.

Assessment should therefore combine an examination of technical provenance with ordinary principles of relevance, context, credibility, and reasonable doubt. Expert testimony should illuminate the scientific and technological questions, not replace legal reasoning. In a system of freely evaluated evidence, a court can take digital material into account when convinced of its reliability, but it should be able to explain why competing interpretations or documented defects do not undermine the conclusion reached.

The French requirement that evidence be presented and debated before the court and the United States' distinction between authentication and other grounds of objection demonstrate that different legal traditions recognise a continuing judicial responsibility to test electronic proof.[23] The lesson for comparative reform is that the criminal court must have both the legal power and the practical capacity to evaluate contested technical evidence.

B. Fair-trial guarantees and effective challenge

The rights implications of digital evidence are not limited to the privacy interests implicated by collection. Fairness also concerns the opportunity to examine the material used to establish criminal responsibility. If the prosecution relies upon a forensic conclusion without disclosing enough information for its basis to be tested, the defence may face a substantial informational disadvantage. Effective challenge can require access to the relevant files or a forensic copy, an intelligible expert report, appropriate technical assistance, and a judicial procedure for resolving disputes about protected or sensitive data.

Disclosure need not be unlimited. Personal information belonging to third parties, confidential sources, and legitimate security concerns may require protective arrangements. However, confidentiality restrictions must not render material evidence effectively immune from challenge. The decisive principle is procedural fairness: a party should have a meaningful opportunity to contest the evidential propositions on which the opposing party relies, under controls proportionate to legitimate competing interests.

These concerns are magnified when digital searches retrieve large volumes of irrelevant records or information whose significance depends on proprietary software. Courts should be alert to claims of absolute technological certainty and should demand clear explanations of error risks,

[23] CODE DE PROCÉDURE PÉNALE [C. pr. pén.] art. 427 (Fr.), https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037108959/2026-01-15; Fed. R. Evid. 902(14) advisory committee's note to 2017 amendment.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

methodological assumptions, and the connection between the technical finding and the legal element allegedly proved.

C. Cross-border evidence and international cooperation

Criminal investigators frequently seek data held by a service provider outside the investigating state. The legal problem is not resolved by the ability to access a server remotely. Competing questions arise concerning territorial authority, provider obligations, the legal classification of data, secrecy rules, privacy protections, and the admissibility of information received through international assistance. Delay can result in deletion or routine overwriting; excessive haste can undermine lawful cooperation and individual rights.

The Budapest Convention and the EU's production and preservation order framework offer examples of how legislatures can distinguish emergency preservation from subsequent disclosure, allocate responsibilities, and establish mechanisms for challenge.[24] For the UAE and other non-EU jurisdictions, these approaches are relevant as comparative models rather than directly applicable prescriptions. Domestic law, applicable treaties, and established international cooperation channels must determine the lawful path for obtaining particular records.

Effective reform should combine rapid preservation mechanisms, clearly identified competent authorities, reliable channels of contact with foreign providers, and judicially supervised access where the degree of intrusion requires it. Cooperation should also support the transfer of material in a form that preserves relevant metadata and permits the receiving authority to verify authenticity. International assistance is valuable only if the resulting evidence can withstand scrutiny at trial.

VII. Findings and proposed legal reforms

A. Principal findings

The doctrinal and comparative analysis supports five findings. First, the legal recognition of digital evidence has progressed more quickly than the development of uniform procedures for documenting its technical lifecycle. Second, the admissibility and probative strength of electronic records cannot be assessed without addressing both the lawfulness of acquisition and the integrity of the resulting data. Third, the chain of custody is not simply an administrative form: it is a means of making evidential continuity traceable and open to examination. Fourth, the forensic expert plays an essential explanatory role but does not displace the criminal judge's

[24] Convention on Cybercrime, *supra* note 9, arts. 16–19; Regulation (EU) 2023/1543, *supra* note 14, arts. 1, 18, 34.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

responsibility to evaluate proof. Fifth, transnational data storage has made cooperation procedures central to the practical effectiveness of criminal investigation.

The UAE's express statutory recognition of technical searches provides an important foundation, especially when Article 73 is read alongside the safeguards governing monitoring and the protection of lawyer-client material. The analysis nevertheless identifies areas where more detailed procedural guidance may improve consistency and transparency: standards for documenting extractions, preservation of metadata, the handling of privileged information, disclosure of forensic methods, and independent testing of contested findings. These are reform proposals grounded in doctrinal comparison, not findings that a particular UAE institution has failed to comply with existing law.

B. An integrated three-stage test

This study proposes a three-stage evaluative framework suitable for guiding legislative drafting and judicial analysis. The first stage is lawfulness: the investigator must identify the competent authority, lawful purpose, appropriate authorisation, and applicable limits on search, monitoring, seizure, and disclosure. The second is integrity: records should demonstrate a credible connection between the collected source and the exhibit presented, supported by a documented chain of custody, appropriate forensic methods, and explanation of uncertainties. The third is contestability: a court must ensure that the parties can meaningfully scrutinise the evidence, challenge the forensic account, and debate its probative significance within the applicable fair-trial framework.

These stages should not be treated as a substitute for any national statute or as a claim that every legal system employs identical exclusionary remedies. Rather, they form an analytical discipline for asking different kinds of questions that may otherwise be conflated. A perfectly matched hash value does not cure an unlawful interception; a lawful search authorisation does not cure an unreliable extraction; and apparent technical reliability does not eliminate the need to examine the accused person's competing explanation.

C. Procedural, institutional, and legislative recommendations

First, legislative or authoritative procedural guidance should specify minimum requirements for identifying, obtaining, preserving, transferring, and examining digital evidence. Rules should distinguish stored content, communications interception, subscriber data, traffic data, and remotely held information to the extent required by applicable legal protections. Second, digital chain-of-custody records should be standardised, with clear responsibility for each

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

acquisition, transfer, examination, and authorised access. Appropriate integrity checks and secure storage practices should be documented rather than merely asserted.

Third, forensic examination should be supported by demonstrable competence, quality-assurance processes, and transparent reporting standards. Courts and prosecutors would benefit from training that enables them to ask informed questions about timestamps, account attribution, volatile data, cryptographic verification, tool limitations, and conflicting forensic interpretations. Fourth, procedures should permit proportionate examination by the defence while respecting privilege, third-party privacy, and legitimate confidentiality interests. Where direct disclosure is not possible, courts should consider safeguards that preserve meaningful adversarial testing.

Fifth, the state should continue developing practical cooperation mechanisms for rapidly preserving and lawfully obtaining cross-border records. Such mechanisms should define competent authorities, documentary requirements, secure transfer practices, and available legal remedies. Finally, law reform should be accompanied by continuing research into emerging challenges, including cloud computing, encrypted services, and new forms of automatically generated information. The objective is not a technology-specific catalogue likely to become obsolete, but a durable statutory and procedural framework that adapts to technical change without compromising justice.

VIII. Conclusion

Digital evidence has become an indispensable component of criminal investigation and adjudication, but its evidential importance cannot be measured by technological sophistication alone. The central legal problem is no longer merely whether electronic material can be recognised as evidence. It is whether that material is acquired under lawful authority, preserved and interpreted through reliable procedures, and subjected to effective judicial and adversarial scrutiny. Those requirements are cumulative: a weakness at any stage can undermine confidence in the final evidential inference.

The selected comparative examples reveal complementary solutions. The Budapest framework emphasises preservation and cooperation; European developments illustrate formalised cross-border mechanisms and rights-sensitive procedures; United States evidence rules distinguish authentication from broader admissibility; and the UAE Criminal Procedures Law expressly provides for technologically mediated searches and safeguards relating to communications and defence material. The analysis supports more precise procedural standards, stronger forensic documentation, competent independent assessment, and practical arrangements for

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

transnational data exchange. The proposed synthesis of lawfulness, integrity, and contestability offers an organising principle for those reforms. Criminal justice systems can benefit from digital technology only when its capabilities remain subject to law, forensic transparency, and the guarantees of a fair trial.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]