JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 3, Issue 1 (2025) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2025/3/1/11

Digital Footprints as Forensic Evidence in Criminal Justice: Scientific Foundations, Evidentiary Reliability, and Emerging Challenges

Prof. Laura Brian[1], Holy Hemmings[2], Lin Quan Tao[3]

[1] *Professor, Department of Computer Sciences, Brisbane University, U.K.*

[2] *Associate Professor,School of Law, Brisbane University, U.K*

[3] *Associate Professor, Department of Law, University of Sungkyunkwan, Korea*

Received: 20 March 2025 **Revised:** 19 May 2025 **Accepted:** 19 July 2025 **Published:** 29 September 2025

ABSTRACT

The increasing digitisation of social, economic and personal activity has transformed the nature of criminal investigation. Computers, smartphones, cloud platforms, social-media applications, connected vehicles, wearable devices, online banking systems, surveillance systems and Internet services continuously generate traces capable of reconstructing human activity. These traces, commonly described as digital footprints, have consequently become an important component of contemporary forensic investigation. Unlike conventional physical evidence, digital footprints are often dynamic, distributed across multiple devices and jurisdictions, generated automatically by software, and capable of being modified, overwritten, encrypted or deleted. Their evidentiary significance therefore depends not simply upon their existence but upon the scientific reliability of the processes through which they are identified, acquired, preserved, interpreted and attributed to a particular person or event. This article examines the scientific foundations of digital footprints as forensic evidence and analyses the principal challenges surrounding their evidentiary reliability in criminal justice. Particular attention is given to metadata, timestamps, IP addresses, geolocation, browser artefacts, application databases, mobile-device records, cloud data, social-media traces, network logs and deleted information. The article adopts a science-centred approach while examining the interaction between forensic methodology and legal standards of admissibility, authenticity, integrity and probative value. Evidence from the National Institute of Standards and Technology indicates that digital investigation techniques are fundamentally grounded in established computer-science principles, while simultaneously recognising limitations arising from rapidly changing software, incomplete acquisition and interpretation of artefacts. Real-world data demonstrate the growing scale of digital crime and the increasing importance of electronically stored information in investigations. The article argues that the principal challenge is no longer whether digital footprints can constitute evidence, but whether forensic practitioners can demonstrate sufficient scientific reliability concerning provenance, integrity, reproducibility, attribution and interpretation. It proposes a strengthened framework based upon validated forensic tools, transparent methodologies, cryptographic integrity verification, reproducibility, quality assurance, probabilistic interpretation and scientifically informed judicial evaluation. The paper concludes that the future credibility of digital evidence depends upon treating digital footprints not merely as technological records but as forensic traces requiring scientifically defensible interpretation.

Keywords: *digital footprints, digital evidence, digital forensics, forensic science, evidentiary reliability, authentication, metadata, cybercrime.*

1. Introduction

The modern individual leaves a continuous trail of electronically generated information. A smartphone records connections with cellular networks, applications generate event logs, websites register access, cloud services maintain authentication histories, navigation systems record locations, cameras capture images and financial platforms preserve transaction histories. These records are produced frequently without deliberate action by the user. As a result, contemporary criminal investigation increasingly encounters evidence that does not exist in the traditional form of a document, weapon, fingerprint or biological specimen but as a sequence of digital traces distributed across devices, applications and networks. The National Institute of Standards and Technology (NIST) describes digital evidence broadly as information contained in computers, mobile devices and associated audio, video, image, software and hardware systems, and recognizes digital forensics as the retrieval, storage and analysis of electronic information relevant to criminal investigation (NIST, 2024). The importance of this development is reflected in the scale of contemporary Internet-related crime. The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) recorded 880,418 complaints and more than US$12.5 billion in reported losses in 2023, representing approximately a 10% increase in complaints and a 22% increase in losses compared with 2022 (Federal Bureau of Investigation [FBI], 2024). The 2024 IC3 report recorded 333,981 cyber-enabled fraud complaints involving approximately US$13.7 billion in reported losses, accounting for about 83% of all reported IC3 losses that year (FBI, 2025). Although these figures represent reported complaints rather than the total incidence of cybercrime, they illustrate the enormous evidentiary environment generated by digitally mediated criminality. Digital footprints have therefore become relevant not only to specifically cyber-dependent offences but also to conventional crimes. A homicide may leave location records, messages, photographs and search histories; a financial crime may generate authentication logs and transaction metadata; trafficking investigations may depend upon encrypted communications and platform records; and organized crime investigations may rely upon patterns linking multiple devices and accounts. The scientific problem begins with the nature of the trace itself. A digital footprint is not necessarily a direct representation of human behavior. It is usually an artefact produced by a technical system. A timestamp may reflect a device clock rather than actual event time; an IP address may identify a network endpoint rather than an individual; a geolocation coordinate may have varying levels of accuracy; a deleted database record may be reconstructed imperfectly; and a social-media account may be controlled by a person other than the registered user. The forensic significance of a digital footprint therefore depends upon the relationship between the underlying event, the technological system that recorded it, the process used to retrieve it and the inference ultimately presented to the court. This distinction is central to scientific reliability. NIST's Digital Investigation Techniques: A NIST Scientific Foundation Review concluded that digital investigation techniques rest upon established computer-science principles and can be reliable when appropriately applied, but it also identified important limitations: investigators may fail to discover all relevant evidence, recovery of deleted information may produce extraneous material, and changes in operating systems and applications can alter the meaning of digital artefacts (Lyle et al., 2022).

Consequently, the central issue for criminal justice is not simply whether digital information is available. The more difficult question is whether a particular digital trace can be scientifically connected to a particular event, device or person with a degree of reliability sufficient to support a legal conclusion. Traditional forensic science has developed around concepts such as observation, measurement, reproducibility, validation, error and interpretation. Digital forensics increasingly requires the same intellectual discipline. The field cannot rely solely on the apparent precision of computer-generated records because technical precision does not automatically establish evidentiary truth. A database can accurately report what its software recorded while the underlying record may still be incomplete or wrongly attributed. Digital footprints should consequently be understood as forensic traces: observable remnants of activities whose meaning must be reconstructed through scientifically controlled processes. This article examines that proposition through six interconnected dimensions: the scientific nature of digital footprints; the principal categories and formation mechanisms of digital traces; forensic acquisition and preservation; reliability, authentication and attribution; legal challenges surrounding admissibility and privacy; and the development of a scientifically stronger framework for digital evidence in international criminal justice.

2. Scientific Foundations and Taxonomy of Digital Footprints

The scientific character of digital-footprint evidence begins with understanding how digital traces are generated. Unlike many physical traces, digital traces are produced through interactions between hardware, operating systems, applications, networks and users. Every layer can generate information independently. An operating system may record file creation and modification events; a web browser can retain history, cache and cookies; an application may maintain databases containing messages or activity records; a cellular network may generate connection records; and a cloud platform may retain authentication and access logs. These records can subsequently interact, allowing investigators to reconstruct sequences of activity. NIST's scientific foundation review identifies the examination of digital evidence as fundamentally dependent upon established computer-science operations, including copying data, searching data, examining timestamps and retrieving application or communication records (Lyle et al., 2022). The first major category is **device-generated evidence**. Computers and smartphones may contain files, deleted files, system logs, application databases, browser records, messages, photographs, contact lists and authentication information. Mobile devices are particularly valuable because they combine communication, location, photography, financial activity, Internet access and authentication functions. NIST's mobile-forensics guidance describes the forensic process as involving validation, preservation, acquisition, examination, analysis and reporting, demonstrating that extraction is only one component of the scientific process (Ayers et al., 2014). The second category is **network-generated evidence**. IP addresses, network logs, Domain Name System queries, firewall records, routing information and authentication events may reveal connections between devices and online services. Such information can establish that a device or network endpoint communicated with a particular server at a particular time. However, it normally cannot independently establish who physically operated the device. Network address translation, shared networks, virtual private networks, public Wi-Fi, proxy systems and compromised devices complicate attribution. The third category is **application and platform evidence**. Social-media platforms,

messaging applications, online marketplaces and financial services create extensive records concerning accounts, sessions, messages, uploads, interactions and transactions. These records may be particularly powerful when multiple independent systems produce mutually consistent traces. Their scientific value, however, depends upon understanding the platform's data-generation architecture and retention policies. The fourth category is **metadata**. Metadata describes information about data rather than necessarily the substantive content itself. A photograph may contain capture time, device information and geographical coordinates; a document may include creation and modification information; and an email may contain routing headers. Metadata can be extremely valuable for reconstructing chronology and provenance, but it must not be treated as inherently accurate. System clocks can be incorrect, metadata can be modified, synchronization mechanisms can introduce discrepancies and software may transform or remove fields. The fifth category consists of **location footprints**. Smartphones can generate location information through global navigation satellite systems, cellular networks, Wi-Fi positioning and application-specific sensors. The scientific interpretation of location evidence requires attention to measurement uncertainty. A coordinate does not necessarily indicate that an individual was physically standing at that exact point. It may represent a calculated location, an associated network location or an application-specific estimate. The sixth category is **cloud and distributed evidence**. Increasingly, relevant information is not stored on a single physical device but distributed among cloud servers, synchronized devices and geographically separated data centers. This creates significant forensic advantages because deleted or unavailable local information may remain accessible elsewhere. At the same time, it complicates provenance, jurisdiction, preservation and acquisition. ISO/IEC 27037:2012 establishes guidance for the identification, collection, acquisition and preservation of potential digital evidence and specifically recognizes storage media, mobile devices and related digital environments (International Organization for Standardization [ISO], 2012). The scientific importance of this taxonomy lies in the principle of **independent corroboration**. A single digital trace may be ambiguous, but multiple traces generated through technically independent mechanisms can substantially strengthen an inference. For example, an alleged online transaction may be supported by a device record, server log, authentication record and financial transaction. The forensic question becomes whether these records converge on a common explanation. This approach resembles traditional forensic reasoning in which different forms of evidence are assessed for consistency. Digital evidence, however, introduces an additional difficulty: many traces are generated by deterministic software rather than directly by human action. A forensic examiner must therefore understand the technical pathway between behavior and recorded artefact. Scientific competence in digital forensics consequently requires more than familiarity with forensic software. It requires knowledge of operating systems, databases, file systems, networking, cryptographic functions, and application architecture and data structures. The scientific foundation of digital footprints rests upon this technical understanding. Without it, investigators risk confusing the existence of a record with the truth of the proposition inferred from that record.

3. Acquisition, Preservation, Validation, and Forensic Integrity

The reliability of a digital footprint begins before its interpretation. Evidence that is improperly acquired may be scientifically compromised even if the subsequent analysis is technically sophisticated. Digital information is unusually vulnerable because ordinary interaction with a device can alter its contents. A smartphone may receive new messages, update applications, change temporary files or alter system logs. A computer may automatically modify access timestamps or overwrite deleted information. Cloud data may change continuously while an investigation is being conducted. Consequently, forensic acquisition must seek to preserve the evidentiary state while creating a reproducible basis for examination. NIST's mobile-device guidance explicitly identifies preservation and acquisition as core stages of forensic examination (Ayers et al., 2014). ISO/IEC 27037 similarly focuses upon identification, collection, acquisition and preservation because these activities establish the foundation for subsequent analysis (ISO, 2012). A central scientific technique is the creation of a forensic copy or image that can be examined without repeatedly manipulating the original source. Cryptographic hashing can then be used to generate a fixed-length representation of the acquired data. If the same hash value is obtained from the source and its forensic copy under appropriate conditions, the result provides evidence that the copied data correspond to the source at the relevant stage. Hashing, however, should not be misunderstood as proof that the underlying data are truthful. It establishes integrity of a particular digital representation, not the accuracy of the information originally recorded by a device or service. This distinction is critical. If a malicious actor altered a file before investigators acquired it, a perfect hash of the altered file would merely prove that the copy accurately reflects the already altered source. Scientific reliability therefore requires a chain extending from acquisition to interpretation. Documentation is equally important. Investigators should record the identity and condition of devices, acquisition methods, software versions, tools used, relevant settings, hash values, dates, times and persons involved in handling evidence. The objective is reproducibility: another competent examiner should be able, within reasonable limits, to understand what was done and evaluate whether the conclusion follows from the data. NIST emphasizes that digital evidence preservation presents problems beyond conventional evidence because digital objects may be easily altered and may exist in complex technological environments (Guttman et al., 2022). The problem becomes particularly difficult when proprietary forensic tools are used. Commercial extraction systems may process large amounts of data efficiently, but investigators and courts may not always have complete knowledge of the algorithms through which information is extracted or reconstructed. A tool may parse an application database, recover deleted information or translate proprietary formats. If the underlying process is poorly validated, a visually persuasive report can conceal methodological uncertainty. The scientific community has therefore increasingly emphasized tool testing and validation. NIST maintains forensic testing programmes and reference datasets precisely because forensic conclusions depend upon the performance of technical tools as well as examiner competence (NIST, 2024). Validation must also account for technological change. Applications are updated frequently, operating systems change database structures and security features evolve. NIST's scientific foundation review specifically warns that the meaning and significance of digital artefacts can change as software is revised (Lyle et al., 2022). Thus, a forensic method validated for one application version cannot automatically be assumed to perform identically with another. Another important issue

is the recovery of deleted information. Deleted data may persist in unallocated storage, application databases, backups or cloud systems. Yet recovery processes can produce fragments that lack sufficient context. A recovered text string does not necessarily establish that the entire original message existed in the reconstructed form. Fragmentation, database remnants and partial overwriting can produce misleading associations. NIST accordingly notes that recovery of deleted files can produce extraneous material (Lyle et al., 2022). Scientific reporting should therefore distinguish clearly between **observed artefacts**, **technical interpretations**, and **investigative conclusions**. For example, the statement "the device contained a browser record showing access to a website at 22:15" is fundamentally different from the conclusion "the accused accessed the website at 22:15." The first describes an artefact; the second attributes an action to a person. The evidentiary distance between them must be justified. Strong digital-forensic practice therefore requires methodological transparency, validated tools, controlled acquisition, integrity verification, complete documentation and cautious interpretation. These principles transform digital evidence from raw electronic information into scientifically defensible forensic evidence.

4. Reliability, Authentication, Attribution, and Interpretation of Digital Traces

The most difficult scientific question in digital-footprint evidence is usually not whether a record exists but what the record proves. Reliability has several distinct dimensions: **existence, integrity, provenance, temporal accuracy, contextual meaning and attribution**. A digital record may satisfy one dimension while failing another. A server log, for example, may be authentic and accurately preserved while still failing to establish which individual controlled the device associated with the logged activity. Authentication therefore has to be separated from attribution. Authentication asks whether the digital record is what it purports to be. Attribution asks whether the activity represented by the record can reasonably be associated with a particular person. This distinction becomes particularly important with IP addresses. An IP address generally identifies a network interface or connection endpoint rather than a human actor. Shared networks, dynamic addressing, NAT, public Wi-Fi, corporate systems and compromised devices can all create circumstances in which multiple users appear through the same address. Consequently, an IP address can be a valuable investigative lead without necessarily being conclusive evidence of individual conduct. The same problem appears with user accounts. A social-media account may be registered to a person but accessed by another person, compromised by an attacker or operated through a shared device. Attribution therefore requires corroboration. Device identifiers, authentication records, location information, message history and independent witness or physical evidence may collectively strengthen the inference. **Temporal interpretation** is another major source of error. Digital systems use different time zones, clock settings and synchronization mechanisms. Some records record creation time, others modification time, access time, server time or application-specific event time. An investigator who treats every timestamp as a direct representation of real-world time risks constructing an incorrect chronology. A scientifically defensible timeline should identify the source of each timestamp and account for clock drift, time-zone conversion, daylight-saving effects where applicable, synchronization and differences between device and server clocks. Digital footprints are therefore best understood probabilistically rather than as mechanically conclusive facts. A forensic conclusion should

reflect the strength of competing explanations. Suppose a smartphone contains location records placing the device near a crime scene. The scientific inference is that the device was likely within the relevant location range at the recorded time, subject to the accuracy and provenance of the location system. The stronger proposition, that the accused personally possessed the phone and committed the offence, requires additional evidence. This distinction reflects a broader principle in forensic science: evidence does not ordinarily speak for itself; its value depends upon the propositions being evaluated and the probability of alternative explanations. The OSAC/NIST framework for digital and multimedia evidence emphasizes that forensic science involves using scientific reasoning and processes to answer questions associated with specific events and legal contexts (Pollitt et al., 2019). The framework's emphasis on traces is particularly relevant because digital evidence should be interpreted as an observable trace from which competing explanations are evaluated. **Reproducibility** is equally important. If two qualified examiners use appropriately validated methods on the same evidentiary material, they should be capable of reaching substantially consistent observations. This does not mean that every interpretative conclusion must be identical. Some digital-forensic questions are inherently inferential, particularly attribution and intent. The scientific objective is therefore not artificial certainty but transparent reasoning and controlled uncertainty. **Tool reliability** presents another challenge. Forensic software can automate extraction, categorization and analysis, but automation may conceal assumptions. Tools can parse artefacts incorrectly, fail to support new application versions or generate different outputs depending upon configuration. Independent verification and cross-tool comparison can reduce these risks. NIST's scientific foundation review concluded that the basic techniques underlying digital investigation are sound while recognizing that technological change and incomplete evidence impose limitations (Lyle et al., 2022). Finally, the emergence of artificial intelligence introduces a new layer of complexity. Machine-learning systems may be used to classify images, identify patterns, reconstruct deleted information or priorities relevant material within enormous datasets. These applications can improve investigative efficiency, but their outputs may not always be readily interpretable. If an AI system identifies a pattern within digital evidence, the forensic examiner must distinguish between the machine-generated classification and the underlying observations supporting the conclusion. The use of AI should therefore complement rather than replace scientifically transparent forensic examination. Digital evidence becomes most reliable when its conclusions are proportionate to the quality of the underlying trace, the validity of the method and the uncertainty surrounding attribution.

5. Evidentiary Admissibility, Privacy, and Cross-Border Challenges

Scientific reliability and legal admissibility are related but distinct questions. Science asks whether a method produces reliable knowledge; law determines whether and under what conditions that knowledge may be presented to a court. Across jurisdictions, rules differ regarding authenticity, hearsay, relevance, expert testimony, chain of custody, search and seizure, privacy and electronic communications. Yet several common principles emerge: the evidence should be relevant, authentic, sufficiently reliable, lawfully obtained and capable of meaningful evaluation by the opposing party. Digital footprints create particular challenges because their quantity can be enormous and their origin may be distributed across multiple

jurisdictions. The 2024 SIRIUS EU Electronic Evidence Situation Report observed that criminal investigations and prosecutions increasingly depend upon access to electronic evidence and highlighted the practical difficulties surrounding cross-border access to digital information (Europol, 2024). Cloud computing intensifies this problem because data relating to a single user may be processed or stored in several countries. An investigator may possess lawful authority in one jurisdiction while the relevant provider stores the information in another. Different privacy regimes, data-retention rules and procedural requirements can consequently affect the availability and admissibility of evidence. The scientific chain of custody also becomes more complex. Evidence acquired directly from a seized device differs from information supplied by a service provider. In the latter case, investigators must establish the provider's record-generation procedures, preservation systems and methods of authentication. A court may reasonably ask how the record was created, who controlled the system, whether the system was operating normally and whether the record could have been altered. **Privacy** creates another tension. Digital devices frequently contain information far beyond the scope of the suspected offence. A smartphone may reveal medical information, intimate communications, financial records, religious activities, professional relationships and information concerning third parties. From a forensic perspective, comprehensive extraction may appear efficient, but from a constitutional and human-rights perspective, indiscriminate examination can become disproportionate. Scientific capability does not itself establish legal necessity. The greater the capacity of forensic technology to reconstruct a person's life, the greater the need for legal limits on collection, retention and secondary use. The principle of data minimization is therefore relevant even in criminal investigation. Investigators should seek information reasonably connected to the investigative purpose and protect unrelated personal information where feasible. Encryption presents a further challenge. Strong encryption can protect legitimate privacy and security while simultaneously limiting investigators' ability to access relevant evidence. Conversely, techniques that weaken encryption may expose the wider population to security vulnerabilities. The criminal-justice system must therefore avoid treating technological circumvention as an uncomplicated solution. **Authenticity** remains particularly important for social-media evidence. Screenshots can be useful investigative material but may lack information concerning provenance, original metadata or the underlying platform record. A screenshot showing a message does not necessarily establish who created it, when it was created or whether the content was edited. Stronger evidence may include platform records, account logs, original files and independently verified metadata. The scientific hierarchy should therefore distinguish between original or provider-generated records and secondary representations. **Deepfakes and synthetic media** create an emerging challenge. Digital images, audio and video can now be manipulated with increasing sophistication. The traditional assumption that a digital recording represents what occurred is becoming scientifically unsafe. Authentication may require examination of file structure, compression patterns, metadata, provenance information, device characteristics and inconsistencies within the content itself. NIST's digital and multimedia evidence programme recognizes multimedia forensics and deepfake-related research as growing areas of forensic science (NIST, 2024). Courts will consequently need increasingly sophisticated approaches to expert testimony. The appropriate question should not simply be whether an expert is experienced in digital forensics, but whether the method used is scientifically supported,

validated, reproducible and appropriately applied to the particular evidence. International criminal justice additionally requires mechanisms for cooperation, standardization and mutual recognition. ISO/IEC 27037 is significant because it facilitates consistent handling of digital evidence and the exchange of evidence between jurisdictions (ISO, 2012). However, technical standards cannot by themselves resolve differences in substantive law. The future of electronic evidence therefore requires closer integration between forensic science, procedural law, privacy law and international cooperation. The objective should be neither unrestricted investigative access nor excessive procedural barriers. It should be a system in which scientifically reliable evidence can be obtained through lawful, proportionate and transparent procedures.

6. Toward a Scientifically Stronger Framework for Digital Footprint Evidence

The increasing dependence of criminal justice on digital footprints requires a shift from technology-centered investigation toward **science-centred digital forensics**. The first requirement is standardization. Investigative agencies should adopt internationally recognized procedures for identification, acquisition, preservation, examination and reporting. ISO/IEC 27037 provides an established foundation for the early stages of evidence handling, while NIST guidance provides detailed approaches to digital and mobile forensic processes (ISO, 2012; Ayers et al., 2014). The second requirement is systematic validation. A forensic tool should not be treated as reliable simply because it is commercially popular or widely used. Its performance should be evaluated against known datasets, controlled test conditions and relevant versions of operating systems and applications. Validation should identify both false-positive and false-negative risks. The third requirement is transparency. Forensic reports should identify the source of each significant artefact, the method through which it was acquired, the tools and versions used, relevant limitations and the inferential steps leading to the conclusion. Courts should be able to distinguish between what the examiner directly observed and what the examiner inferred. The fourth requirement is reproducibility. Original evidence should be preserved wherever possible, while forensic working copies should be independently verifiable. Hash values, acquisition logs and complete documentation should allow subsequent examination without unnecessary alteration of the source. The fifth requirement is **probabilistic and proposition-based interpretation**. Instead of asserting that a digital footprint "proves" an individual's conduct without qualification, forensic experts should identify the proposition supported by the evidence and consider plausible alternatives. For example, a device location record may support the proposition that the device was in a particular area at a particular time, but attribution to a person may require additional evidence. This distinction can substantially improve the intellectual quality of expert testimony. The sixth requirement is continuous professional competence. Because applications, operating systems, encryption systems and cloud architectures change rapidly, digital forensic expertise cannot remain static. NIST's scientific foundation review specifically identifies technological change as a major limitation because artefact meaning can change when software systems are revised (Lyle et al., 2022). Training must consequently combine computer science, forensic methodology, evidence law, statistics, and cybersecurity and privacy principles. The seventh requirement concerns **quality assurance and independent review**. Major criminal investigations should, where feasible, include peer review of

significant forensic conclusions, especially where digital evidence forms a central part of the prosecution case. Independent examination can reveal extraction errors, misinterpreted timestamps, unsupported attribution and overstatement of certainty. The eighth requirement is stronger governance of cloud and platform evidence. Service providers should maintain auditable mechanisms for preservation and authentication while respecting privacy and applicable law. Standardized formats for provider-generated records could facilitate cross-border use and reduce disputes over authenticity. The ninth requirement is responsible use of artificial intelligence. AI can assist in searching large forensic datasets, clustering related artefacts, identifying anomalous activity and prioritizing evidence. However, automated conclusions should remain subject to human verification and documented validation. The system should not be treated as an infallible forensic authority. The tenth requirement is privacy protection. Because digital forensic tools can reconstruct extraordinarily detailed aspects of individual behavior, legal frameworks should require proportionality, purpose limitation, secure retention and controlled access. Finally, international cooperation should be strengthened through common terminology, compatible technical standards and procedures for cross-border preservation and transfer. The growing importance of electronic evidence is already recognized at the international level; the 2024 SIRIUS report demonstrates the continuing need to reconcile law-enforcement requirements with the technical and legal complexity of electronic evidence access (Europol, 2024). The broader objective should be the creation of an international **digital evidence reliability framework** based on five principles: scientific validity, integrity, provenance, reproducibility and proportionality. Such a framework would not require identical evidence laws across countries. Instead, it would establish a common scientific baseline against which digital evidence can be evaluated. The transformation of digital footprints into trustworthy forensic evidence depends ultimately upon recognizing that technological availability is not equivalent to evidentiary reliability. The more powerful digital forensic technology becomes, the greater the need for scientific discipline in its application.

7. Conclusion

Digital footprints have become an essential component of contemporary criminal investigation because modern human activity is increasingly mediated through digital systems. The scale of the phenomenon is illustrated by the FBI's 2023 record of 880,418 Internet-crime complaints and more than US$12.5 billion in reported losses, followed by approximately US$13.7 billion in cyber-enabled-fraud losses reported in 2024 (FBI, 2024, 2025). Yet the growing availability of digital traces does not automatically make them reliable evidence. Digital footprints are technical artefacts generated through complex interactions between users, devices, software, networks and service providers. Their forensic value depends upon scientifically defensible acquisition, preservation, validation, interpretation and attribution. The scientific foundations of digital forensics are substantial. NIST's scientific foundation review concluded that digital investigation techniques are based upon established principles of computer science and can be reliable when appropriately applied, while also identifying limitations arising from incomplete evidence, deleted-data recovery and technological change (Lyle et al., 2022). This balanced position is important for the future of criminal justice. Digital evidence should neither be regarded with unwarranted suspicion nor accepted merely because it originates from a

computer system. Its evidentiary strength must be determined through the same scientific principles that increasingly govern other forensic disciplines. The central challenge is attribution. A timestamp does not necessarily establish when a human acted; an IP address does not necessarily identify a person; a device location does not necessarily establish possession; and an account record does not necessarily prove who operated the account. These distinctions require courts and forensic experts to move from simplistic notions of "digital proof" toward structured reasoning about traces, propositions, alternative explanations and uncertainty. The future of digital evidence will also be shaped by cloud computing, encryption, artificial intelligence, connected devices and synthetic media. These technologies will expand the quantity and complexity of digital traces while simultaneously making authentication and interpretation more difficult. The appropriate response is not to restrict technological development but to strengthen forensic science. Validated tools, international standards, transparent methodologies, cryptographic integrity controls, independent review, probabilistic interpretation and privacy-sensitive investigative procedures should become integral components of digital evidence practice. Ultimately, the legitimacy of digital footprints in criminal justice will depend less on the quantity of information they provide than on the quality of the scientific reasoning used to interpret them. Digital footprints can provide extraordinarily detailed reconstructions of human activity, but their power creates a corresponding responsibility. A scientifically grounded system must ensure that technological traces are converted into legal evidence through methods that are demonstrably reliable, transparent, reproducible and proportionate. The future of criminal justice therefore lies not simply in collecting more digital data, but in developing better science for deciding what those data actually mean.

Declarations

Conflict of interest: The author declares that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analysed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.