International Journal of Business, Law and Political Science
Homepage : https://e-journal.antispublisher.org/index.php/IJBLPS
Email : admin@antispublisher.com

e-ISSN : 3032-1123
IJBLPS, Vol. 3, No. 8, August 2026
Page 67-74
© 2026 IJBLPS :
International Journal of Business, Law and Political Science

Problems of Collecting, Preserving and Evaluating Digital Evidence in the Investigation of Cyber Fraud

B. B. Suyunov
Research Institute of Criminology of the Republic of Uzbekistan, Uzbekistan

Check for updates OPEN ACCESS

DOI : https://doi.org/10.61796/ijblps.v3i8.539

Sections Info

Article history:
Submitted: June 05, 2026
Final Revised: June 30, 2026
Accepted: July 16, 2026
Published: August 08, 2026

Keywords:
Digital evidence
Electronic data
Cyber fraud
Expedited preservation
Evidence integrity
Hash value
Chain of custody
Admissibility
ISO/IEC 27037
Cross-border evidence

ABSTRACT

Objective: *The article examines the problems arising at the three stages of handling digital evidence in the investigation of cyber fraud: their collection, preservation, and evaluation.* ***Method:*** *The institution of digital evidence, introduced into the Criminal Procedure Code of the Republic of Uzbekistan by Law No. ZRU-1003 of 21 November 2024, is subjected to comparative analysis with international standards ISO/IEC 27037, NIST SP 800-86, and SWGDE recommendations.* ***Results:*** *The absence in national legislation of a mechanism for the expedited preservation of electronic data, given their volatility, is identified as the principal problem.* ***Novelty:*** *Proposals for eliminating the absence of an expedited electronic data preservation mechanism are advanced through a comparative analysis of Uzbekistan's legal framework and international digital evidence standards.*

INTRODUCTION

In cases of cyber fraud, the centre of gravity of proof lies not in material traces but in the digital environment. This circumstance confronts the investigation with three consecutive tasks unknown to traditional criminalistics: first, obtaining in good time data that is highly volatile and easily destroyed; second, preserving it unchanged in its original state; and third, substantiating its authenticity and reliability in court by means of objective evidence. An error committed in any one of these three tasks leads to consequences that cannot be corrected at the subsequent stage [1].

In legal terms, the situation has changed appreciably in recent years. Law of the Republic of Uzbekistan No. ZRU-1003 of 21 November 2024 introduced into procedural legislation the concept of digital evidence, together with rules governing the procedure for its collection, submission, securing, inspection, verification and evaluation, storage, return and destruction [2]. Resolution No. 24 of the Plenum of the Supreme Court of the Republic of Uzbekistan of 24 August 2018 "On certain issues of the application of the norms of criminal procedure law relating to the admissibility of evidence" was, in turn, brought into line with these innovations by Resolution No. 14 of 23 June 2025. Nevertheless, a number of questions remain open in practice, and it is precisely these that the present article sets out to analyse [3].

The legal definition of digital evidence is given in Article 204² of the Criminal Procedure Code: electronic data containing information about circumstances relevant to the case, including files in electronic form, audio and video recordings, and data stored on the Internet global information network, are deemed to be digital evidence [4]. Electronic data themselves, pursuant to Article 204¹, are data created, processed and stored by means of electronic devices and information systems, as well as through the use of information technologies. The legislator has thereby drawn a distinction between electronic data and digital evidence: the former is objectively existing information, the latter is information that has undergone procedural evaluation and been admitted to the case file [5].

It is expedient to consider the problems arising at the stage of collecting digital evidence through typical initial investigative situations, since each situation determines its own direction for the search for traces [6].

In the first situation, the card to which the victim transferred the funds is known, but its actual holder is not the organiser of the crime. In such a case the relationships between the "drop" (money mule), the organiser, the operator and the person cashing out the funds are examined [7]. The legal foundation of this situation was altered by Presidential Resolution No. PQ-153 of 30 April 2025, which sets the task of establishing administrative and criminal liability for persons who have permitted the use, in the commission of a cybercrime, of a bank card, bank account, SIM card or electronic wallet registered in their own name. Accordingly, the "drop" is no longer merely a tactical notion but possesses an independent subject matter of proof [8].

In the second situation, a telephone number and an account exist, but they are fictitious or registered in the name of another person. Here the device identifier, IP address, geolocation, login history and connections with other accounts are analysed [9]. In the third situation, the website or account is hosted with a provider in a foreign state, and the question of the expedited preservation of the data and their cross-border acquisition comes to the fore. In the fourth situation, the offence is committed by means of a voice, video or fictitious persona generated by artificial intelligence, which calls for examination of the origin of the content, its metadata, traces of editing and the source device [10].

The first task common to all four situations is the complete and prompt receipt of the initial data from the victim. These include the telephone number, the bank card, the transaction identifier, correspondence, the electronic receipt, audio recordings and screenshots, the address of the website or account, the date and exact time of the call, and information about the device on which the harm was inflicted [11]. The receipt of such data must be formalised in accordance with the requirements of Article 201¹ of the Code (submission of electronic data on one's own initiative) and Article 202 (record of submission); under part three of Article 204¹, it must be carried out with the participation of a specialist, and the primary electronic objects must be inspected [12].

The second task of collection is to protect the data from loss. In international practice this task is resolved through a separate procedural institution. Article 16 of the

Council of Europe Convention on Cybercrime provides for the expedited preservation of stored computer data: where there are grounds to believe that the data are vulnerable to loss or modification, the competent authority orders the person in possession of them to preserve them, and subsequently obtains them in the established procedural manner [13]. Articles 29 and 30 of the Convention govern the application of this measure at the international level, while Article 35 establishes a network of 24/7 points of contact for the provision of urgent assistance. Analogous mechanisms — the expedited preservation of electronic data, the partial disclosure of traffic data, and the institution of the production order are likewise enshrined in the United Nations Convention against Cybercrime [14].

RESEARCH METHOD

This study employs a qualitative doctrinal legal research methodology based on the analysis of legislative acts, international legal instruments, and comparative legal approaches relating to digital evidence in cyber fraud investigations. The research examines the provisions of the Criminal Procedure Code of the Republic of Uzbekistan, recent legislative reforms concerning digital evidence, and relevant resolutions of the Supreme Court. International standards, including ISO/IEC 27037, NIST Special Publication 800-86, the Budapest Convention on Cybercrime, the United Nations Convention against Cybercrime, and SWGDE best practice guidelines, are comparatively analyzed to identify similarities and differences between national and international approaches.

The study further applies comparative legal analysis to evaluate procedural mechanisms governing the collection, preservation, and evaluation of digital evidence. Analytical and systematic methods are used to identify legislative gaps affecting the admissibility and integrity of electronic evidence in criminal proceedings. Based on these findings, practical legislative recommendations are formulated to improve the procedural regulation of digital evidence handling in Uzbekistan while ensuring compliance with internationally recognized forensic standards.

RESULTS AND DISCUSSION

Results

The study demonstrates that the recent incorporation of digital evidence into the Criminal Procedure Code of the Republic of Uzbekistan represents a significant advancement in adapting criminal procedure to contemporary cybercrime investigations. Nevertheless, several procedural deficiencies remain unresolved [15].

The analysis identifies the absence of an expedited preservation mechanism for electronic data as the most critical legislative gap. Unlike the Budapest Convention and the United Nations Convention against Cybercrime, the current legislation does not empower investigators to require the immediate preservation of volatile electronic information before it is deleted or altered. This considerably reduces the effectiveness of investigations involving foreign service providers and cloud-based platforms.

The research also reveals that existing procedural provisions regulating the preservation of digital evidence do not establish technical requirements for verifying evidence integrity. Although legislation requires maintaining the integrity and identity of digital evidence, it does not explicitly require the calculation and documentation of cryptographic hash values or standardized chain-of-custody procedures, creating uncertainty regarding evidential reliability.

Furthermore, the evaluation of artificial intelligence-generated content presents new legal challenges that are not sufficiently addressed by current procedural legislation. Existing forensic procedures do not provide specialized methodologies for verifying the authenticity of AI-generated audio, video, or synthetic identities.

Overall, the findings indicate that harmonization of national legislation with internationally recognized digital forensic standards would substantially improve the reliability, admissibility, and effectiveness of digital evidence in cyber fraud investigations.

Discussion

The analysis demonstrates that the introduction of digital evidence into the criminal procedural legislation of the Republic of Uzbekistan has significantly strengthened the legal framework for investigating cyber fraud. Nevertheless, the study reveals that several procedural and technical issues continue to limit the effective collection, preservation, and evaluation of digital evidence. A comparison with international standards, including ISO/IEC 27037, NIST SP 800-86, and the Budapest Convention on Cybercrime, indicates that while the national legislation generally follows internationally recognized principles, it lacks detailed procedural mechanisms for ensuring the integrity and authenticity of digital evidence.

The findings further suggest that the absence of an expedited preservation procedure for electronic data constitutes one of the most significant shortcomings of the current legal framework. Since digital information can be modified or deleted within a very short period, delays in obtaining or preserving electronic evidence may seriously undermine criminal investigations. In addition, the study highlights the need to introduce mandatory cryptographic hash verification, standardized chain-of-custody procedures, and specialized forensic methodologies for examining artificial intelligence-generated digital content. Implementing these measures would improve the admissibility, reliability, and evidentiary value of digital evidence while aligning Uzbekistan's criminal procedure legislation with international best practices in digital forensics.

The Criminal Procedure Code of the Republic of Uzbekistan currently in force contains no independent institution for the expedited preservation of electronic data. Article 175 of the Code permits the requisition of electronic data stored in information systems, on electronic devices and in Internet sources; requisition, however, produces a result only where the data still exist. If the provider deletes the data upon expiry of the retention period, the demand becomes nugatory. In our view, this is one of the most

serious gaps in national procedural legislation, and it should be eliminated by supplementing the Code with a separate article on the order for the preservation of electronic data. Such an article should define the grounds for issuing the order, the procedure for issuing it, its initial duration and the conditions for its extension.

The third task of collection is to obtain financial traces simultaneously with digital ones. Waiting until the offender has been fully identified may result in the funds being withdrawn through a series of accounts; the tracing of the transaction chain, the identification of subsequent recipient accounts, the temporary suspension of the funds and the detection of virtual assets must therefore be carried out in parallel with the investigation. In the report prepared jointly with the Egmont Group and INTERPOL, the FATF specifically emphasises the need, in combating fraud in the cyber environment, to strengthen the mechanisms of financial investigation and asset recovery, to increase the transparency of payments, and to introduce instruments for the suspension and freezing of funds.

At the preservation stage, the requirement of the legislation is formulated in general terms. Under Article 208 of the Code, when material, written and digital evidence is stored and when it is transmitted for expert examination or to another body, measures must be taken to prevent its loss, damage, deterioration, or its being combined or intermixed with other evidence. The article, however, does not indicate what such measures are to consist of, while Article 204² leaves the meaning of the terms "integrity and identity" undisclosed. As a result, integrity is in practice often ensured by a sealed package and an entry in the record, whereas this method is insufficient in relation to a digital object: whether a file copy on a sealed device has been altered can be demonstrated not by a seal but only by mathematical verification.

International standards have resolved this question with precision. Standard ISO/IEC 27037:2012 defines four processes in handling digital evidence identification, collection, acquisition and preservation and three principles: auditability, repeatability and reproducibility. The NIST SP 800-86 methodological guide describes the digital forensic process in four phases collection, examination, analysis and reporting and advances the requirement of maintaining data integrity and a rigorous chain of custody at each phase. In the documents of the Scientific Working Group on Digital Evidence (SWGDE) the underlying rule is formulated still more explicitly: changes introduced into the source data must be minimised so far as possible, and where change cannot be entirely prevented, the process must be documented in such detail as to permit its repetition and the explanation of any artefacts thereby produced.

A comparison of these standards with national legislation shows that the norms of Uzbekistan are not contrary to the international approach in substance, but differ from it in the degree of technical precision. Article 204² permits a copy to be made of digital evidence only where its integrity and identity are preserved, and provides that the possibility of copying is secured by the existence of the original which fully accords with the logic of ISO/IEC 27037. Yet whereas the standard indicates the method by which this correspondence is to be proved, the Code leaves the question open. We therefore

propose supplementing Article 204² with a rule to the effect that each making of a copy of digital evidence and each transfer of such evidence is to be accompanied by the calculation of a cryptographic checksum a hash value and by its entry in the relevant record.

At the evaluation stage, digital evidence is tested against the three traditional criteria of relevance, admissibility and reliability. In cyber fraud cases the content of these criteria is filled out in a distinctive manner.

Two conditions are of decisive importance for the question of admissibility. The first is the requirement of the participation of a specialist laid down in Article 95. The second is the procedure established in paragraph 10 of the Plenum resolution in its new wording: electronic data submitted together with an application or report concerning an offence may be used as admissible evidence only where the persons who submitted them have been identified and where it has been established by whom, when, where and in what circumstances those data were found. A necessary condition for admitting them to the case as digital evidence is the existence of a corresponding decision or ruling issued after an inspection record has been drawn up. Where necessary, an expert examination may be ordered for the resolution of this question.

A new and as yet unresolved problem of evaluation is the verification of content generated by artificial intelligence. In a fraud committed by means of a voice, a video or the image of a fictitious person, the audio or video recording submitted as evidence may itself be a fabrication. In such a case the subject of verification is not the content of the material but its origin: the metadata, the encoding parameters, traces of editing, the file's creation history and the source device are examined. The current list of types of forensic examination does not identify an independent type of examination for such research; we therefore consider it necessary to formalise it as an examination of the authenticity of digital content and to develop the corresponding methodology.

Finally, particular attention should be given to the danger of evaluating digital evidence in isolation. Digital evidence is not by itself always sufficient to support a charge: an IP address or a device identifier indicates that a technical means was used, not that a specific person performed the act. It must therefore be evaluated together with the testimony of the victim, banking data, video surveillance recordings, telephone communications, the conclusions of the examination of the device, the results of searches and the conduct of the suspect. This rule is not novel in procedural terms; in cyber fraud cases, however, the outward persuasiveness of technical evidence sometimes leads to its being treated as absolute, which increases the risk of judicial error.

The analysis conducted has shown that all three stages of handling digital evidence in cyber fraud cases constitute a single continuous process: delay at the collection stage nullifies the very object at the preservation stage, while carelessness at the preservation stage leads to the evidence being ruled inadmissible at the evaluation stage. On this basis, the following proposals are advanced.

First, the Criminal Procedure Code should be supplemented with a separate article on the order for the expedited preservation of electronic data. The article should define

the grounds for issuing such an order, the procedure for serving it on communications operators, Internet providers, banks and digital platforms, its initial duration and the conditions for its extension. This institution has been tested in Article 16 of the Budapest Convention and in the corresponding norms of the United Nations Convention, and its incorporation into national legislation would also create a foundation for future international cooperation.

Second, Article 204² should be supplemented with a rule providing that each making of a copy of digital evidence and each transfer of such evidence be effected together with the calculation of a cryptographic checksum and its entry in the record, and Article 208 should separately set out the specific requirements for the storage of digital evidence.

Third, a system should be introduced for keeping certified copies of digital evidence in a specialised digital repository in which the hash value, the access history and the range of users are recorded automatically.

CONCLUSION

Fundamental Finding : This study demonstrates that Customer Relationship Management (CRM) is a strategic capability that strengthens customer retention, satisfaction, and long-term relationship quality in ICT service firms. Effective CRM implementation requires an integrated process consisting of customer portfolio analysis, customer intimacy, business network development, value proposition development, and customer life-cycle management, enabling firms to create greater customer value and enhance their competitive position. **Implication :** The findings suggest that ICT service firms should position CRM as a strategic managerial capability by integrating customer data, service processes, communication channels, and relationship-building activities. Aligning CRM with the 7P service marketing mix can improve customer experience, support service innovation, strengthen customer loyalty, and enhance managerial decision-making. **Limitation :** This study is limited to the ICT service sector and employs a qualitative descriptive approach, which provides contextual insights but does not quantitatively assess the long-term impact of CRM on financial performance, customer loyalty, or customer lifetime value. In addition, the role of emerging technologies in CRM implementation is not examined extensively. **Future Research :** Future research should compare CRM implementation across different industries and organizational contexts, investigate the influence of market dynamics, organizational culture, service quality, and the 7P marketing mix on CRM effectiveness, and examine the long-term contribution of CRM to business performance. Further studies should also explore the integration of artificial intelligence, machine learning, data analytics, and automation to enhance CRM personalization, predictive customer insights, and service responsiveness.

REFERENCES

[1] *Criminal Procedure Code of the Republic of Uzbekistan*, Lex.uz. [Online]. Available: https://lex.uz/docs/111460

[2] *On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan Aimed at Improving the System of Handling Digital Evidence*, Law of the Republic of Uzbekistan No. ZRU-1003, Nov. 21, 2024. [Online]. Available: https://lex.uz/docs/7228758

[3] President of the Republic of Uzbekistan, *On Measures Aimed at Further Strengthening Activities to Combat Crimes Committed with the Use of Information Technologies*, Resolution No. PQ-153, Apr. 30, 2025. [Online]. Available: https://lex.uz/docs/7511145

[4] Plenum of the Supreme Court of the Republic of Uzbekistan, *On Certain Issues of the Application of the Norms of Criminal Procedure Law Relating to the Admissibility of Evidence*, Resolution No. 24, Aug. 24, 2018 (amended by Resolution No. 14, Jun. 23, 2025). [Online]. Available: https://lex.uz/docs/7613615

[5] Council of Europe, *Convention on Cybercrime*, ETS No. 185, Budapest, Hungary, Nov. 23, 2001.

[6] United Nations, *United Nations Convention against Cybercrime*, General Assembly Resolution 79/243, Dec. 24, 2024. [Online]. Available: https://www.unodc.org

[7] *Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, ISO/IEC Standard 27037:2012, International Organization for Standardization, Geneva, Switzerland, 2012.

[8] K. Kent, S. Chevalier, T. Grance, and H. Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2006.

[9] Scientific Working Group on Digital Evidence (SWGDE), "Best practices for computer forensic acquisitions," Doc. 17-F-002-2.1, 2025. [Online]. Available: https://www.swgde.org

[10] Scientific Working Group on Digital Evidence (SWGDE), "Best practices for digital evidence collection," Doc. 18-F-002-2.0, 2025. [Online]. Available: https://www.swgde.org

[11] Scientific Working Group on Digital Evidence (SWGDE), "Best practices for digital evidence acquisition, preservation, and analysis from cloud service providers," Doc. 23-F-004-1.1, 2024. [Online]. Available: https://www.swgde.org

[12] Financial Action Task Force (FATF), Egmont Group of Financial Intelligence Units, and INTERPOL, *Illicit Financial Flows from Cyber-Enabled Fraud*, Paris, France: FATF, 2023.

[13] National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 Rev. 5, Gaithersburg, MD, USA, Sep. 2020.

[14] European Union Agency for Cybersecurity (ENISA), *Guidelines for Securing the Internet of Things*, Heraklion, Greece: ENISA, 2020.

[15] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime*, Vienna, Austria: United Nations, 2013.

B. B. Suyunov
Research Institute of Criminology of the Republic of Uzbekistan, Uzbekistan