The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.06 Issue08 2026
PAGE NO. 97-101
DOI 10.37547/ijlc/Volume06Issue08-17

Judicial and Legal Reforms of New Uzbekistan: From Electronic Traces to Digital Evidence — A New Step in Investigation

Agoyev Shukurullo Safarboyevich
Department of Cyber Law, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent 100197, Uzbekistan

Received: 15 July 2026; **Accepted:** 04 August 2026; **Published:** 28 August 2026

Abstract: The article examines intensive judicial and legal reforms implemented in New Uzbekistan under the leadership of the President, in particular, the digitalization of the criminal process, ensuring transparency and protecting human rights. Based on the Resolution PP-155 (Anti-fraud) and the Law LRU-1003, the concept of 'digital evidence' introduced into national legislation and its practical significance are analyzed. Against the background of guaranteeing individual rights and freedoms, the technical and procedural necessities of conducting investigative actions to obtain samples for forensic examination from digital traces and the requirements of the state standard O‘z DSt ISO/IEC 27037:2017 are systematically studied. As a result, constructive proposals aimed at further improving the quality of judicial and investigative practice and improving legislation based on international standards have been developed.

Keywords: Judicial and legal reforms, New Uzbekistan, digital evidence, digital sampling, Criminal Procedural Code, Anti-fraud system, PP-155, LRU-1003, O‘z DSt ISO/IEC 27037, digital forensics, investigative tactics, forensic activity, information security, human rights guarantee, constructive proposals, procedural legislation, electronic traces.

Introduction:

1. Relevance of the topic and global transformation.

In the modern world, the rapid development of information and communication technologies and digital ecosystems is bringing fundamental changes to all spheres of social relations. The processes of integration and globalization require the transition of public administration and law enforcement activities to a qualitatively new level. In an era where the concept of cyberspace is expanding globally and the virtualization of criminal threats is observed, modernizing traditional forensic methods and evidence bases based on modern digital requirements has become an objective necessity. Analysis of the recent past shows that for many years, national judicial and investigative practice lagged behind rapid technological development to a certain extent, relying more on conservative and paper-based methods. This served as the main factor limiting the speed of identifying transnational crimes committed through information technology and protecting the rights of citizens.

2. Dynamics of reforms in the period of New Uzbekistan.

In the New Uzbekistan, based on the principle "In the name of human honor and dignity," put forward by the head of state Shavkat Mirziyoyev, a new strategic stage has begun for the prompt resolution of organizational, technical, and procedural problems accumulated over years in the judicial system. In order to ensure the rule of law in the country and raise the quality of judicial and investigative work to the level of international standards, important decrees and resolutions were adopted on a systematic basis.

In particular, Decree of the President of the Republic of Uzbekistan No. UP-5441 served to fundamentally improve the activities of judicial and legal bodies [1], Resolutions No. PP-270, No. PP-6256 created a solid foundation for the comprehensive digitalization of

forensic activities, ensuring transparency in the field, and developing non-governmental expert institutions [2;3]. The "Electronic Criminal Proceedings" system, implemented as a logical continuation of these reforms, has eliminated bureaucratic barriers in the processing of criminal cases, minimizing the human factor and corruption risks.

One of the most important steps in the national security system was the Resolution of the Head of State No. PP-155 dated November 30, 2023, "On measures to further improve the system of combating crime in the field of digital technologies," adopted to prevent crimes committed using digital technologies. With this document, the legal framework of the Unified Anti-Fraud System was created to combat theft of funds from bank cards, phishing, and online fraud, and the operational activities of the Cybersecurity Center of the Operational-Search Department of the Ministry of Internal Affairs were transferred to a new methodological basis [4], and the powers to combat crime were slightly expanded.

As a logical continuation of these systemic reforms and with the aim of fundamentally improving personnel development, another important document was adopted by the President of the Republic of Uzbekistan—Resolution No. PP-17 of January 17, 2024, “On Measures to Raise the System of Training, Retraining, and Advanced Training of Personnel for Internal Affairs Bodies to a Qualitatively New Level.” This Resolution marked a fundamental turning point in the training of a new generation of legal professionals and experts capable of countering threats in cyberspace [7].

To ensure the implementation of these strategic objectives, an entirely new system for training qualified specialists with advanced knowledge of modern information technologies, digital forensics, and methodologies for handling digital evidence was introduced at the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan. In particular, specialized departments and digital laboratories were established within the Academy, where trainees began receiving advanced practical and theoretical knowledge on the prompt detection of cybercrimes, secure preservation of electronic traces, and acquisition of digital samples in accordance with international standards. This contributes not only to the development of the legal and technical infrastructure in this field, but also to enhancing the intellectual capacity of personnel necessary to ensure the effectiveness of the reforms.

3. Development of the Legal Framework and Existing Problems

The Law of the Republic of Uzbekistan No. ZRU-1003, adopted on November 21, 2024, should be recognized as one of the most significant milestones of these reforms. For the first time, this Law introduced the concept of “digital evidence” into the Criminal Procedure Code, along with rules governing its procedural consolidation [5]. However, despite this historic legislative development, certain procedural and technical inconsistencies are becoming apparent in practice when carrying out the investigative action of “obtaining samples for examination” (Article 188 of the Criminal Procedure Code) in relation to such digital data.

Our research has revealed that the current provisions of the Criminal Procedure Code do not fully encompass the specific characteristics of the rapidly changing digital environment, such as data stored in volatile memory, cloud servers, and blockchain transactions, nor do they fully incorporate the technical requirements of the state standard O‘z DSt ISO/IEC 27037:2017. An examination of the professional activities of investigators and experts demonstrates that there is a risk of compromising data integrity or remotely deleting data during the acquisition of digital samples.

Therefore, in accordance with the high-level reform concept established by the state, this article aims to provide scientifically and technically substantiated solutions aimed at further improving criminal proceedings through a constructive analysis of existing practical problems.

METHODS

1. Methodological Basis and Analytical Methods of the Study

To address the objectives set within this research, the methods of systemic-structural analysis, comparative legal analysis, forensic-tactical analysis, and logical-legal analysis were employed. In examining the system for transforming electronic traces into legally admissible digital evidence, the current provisions of the Criminal Procedure Code of the Republic of Uzbekistan (CPC), particularly the requirements of Article 188 (“Obtaining Samples for Examination”), were subjected to critical and constructive analysis. During the study, the procedural legislation of leading foreign countries in the field of digital forensics, as well as the practical methodological guidelines of the Department for Combating Cybercrime of the Ministry of Internal Affairs, were comparatively examined.

2. Source Base and Empirical Foundations

To ensure the validity of the scientific conclusions, the technical requirements of the O‘z DSt ISO/IEC

27037:2017 state standard were comprehensively compared with the existing protocols of investigative actions. To strengthen the empirical basis of the research, a questionnaire survey was conducted among 588 practitioners operating throughout the Republic, including inquiry officers, investigators, operational officers, and forensic experts, concerning the technical and legal requirements involved in handling digital evidence and samples. The results obtained were subsequently generalized using statistical methods.

RESULTS

1. Analysis of Objective Practical Needs and Systemic Issues

The results of our research and the surveys conducted demonstrate that, although Presidential Resolution No. PP-155 (Anti-Fraud Resolution) and Law No. ZRU-1003 of 2024 represent revolutionary steps in this field, the need to update national legislation in the technical and procedural chain of obtaining samples from digital traces remains. In particular, 74% of the practitioners who participated in the survey stated that there is currently no unified procedural algorithm for preserving the authenticity of data and ensuring its admissibility and defense in court when obtaining samples from digital devices and virtual environments. The following systemic issues were identified in this area:

. Technical limitations in preserving screen images: The practical guidelines of the Department for Combating Cybercrime of the Ministry of Internal Affairs recommend preserving traces on the Internet by recording the screen together with audio and video (for example, using the Bandicam software) [6, p. 53]. However, the cryptographic integrity (hash value) of the resulting video records or screenshots is not documented in the protocol, which may subsequently give rise to objections concerning the admissibility of such evidence in court proceedings.

. Technical obsolescence in the presentation of digital evidence: Practical guidelines still provide for the use of DVDs when submitting digital data to forensic experts [8, p. 158]. In the era of high-volume cloud data and modern encrypted systems, transferring evidence through such media creates a technical risk of data loss.

. Inconsistency between the state standard and the Criminal Procedure Code: The current O‘z DSt ISO/IEC 27037:2017 standard requires the principle of “non-reversibility” (non-alteration of data) when collecting digital evidence [6, p. 12]. However, Article 188 of the Criminal Procedure Code does not establish a legal mechanism specifying the tactical methods by which an investigator should obtain temporary files stored in the random-access memory (RAM) of a computer or server. Furthermore, although the participation of a specialist is established as a mandatory requirement when obtaining digital evidence, the specific actions that such a specialist must perform are not defined, effectively reducing the specialist to a merely formal participant.

Constructive Solutions: The Author’s Four-Stage Tactical Algorithm

In the course of our research, in order to systematically address the technical and procedural issues identified above and improve the quality of investigations under the conditions of Uzbekistan, we developed the following mandatory four-stage tactical algorithm for obtaining samples from digital traces for forensic examination:

Stage 1: Preservation of RAM (Random-Access Memory) Data. First, a digital copy should be obtained of temporary files, logs, and open chats stored in volatile memory, which may be lost when the device is switched off.

Stage 2: Technical Network Isolation. In order to prevent criminals from remotely deleting or modifying data, the device should immediately be placed in airplane mode or stored in special containers equipped with electromagnetic shielding (Faraday barriers).

Stage 3: Use of “Write-Blocker” Devices. Special “write-blocker” devices that prevent the writing of information should be used on a mandatory basis to ensure that no alterations are made to the system from which the digital sample is being obtained as a result of actions by the investigator or specialist.

Stage 4: Calculation of a Cryptographic Hash Function. To ensure the integrity of the obtained digital sample and its preservation without alteration until it is submitted to the court, its international digital “fingerprint”—an MD5 or SHA-256 hash code—should be calculated and strictly documented in the investigative protocol.

Constructive Proposal for Improving Legislation. In order to ensure the legal force of this tactical algorithm, it is proposed to supplement Article 188 of the Criminal Procedure Code with a new provision allowing digital samples to be obtained through 3D scanning and visual modeling in order to preserve the original state of objects in the virtual environment.

2. Practical and Technical Analysis of the Tactics for Obtaining Digital Samples

In the course of our research, a systematic examination of the practice of documenting crimes committed through information technologies and obtaining digital samples revealed the existence of technical requirements concerning methods for preserving electronic traces in the virtual environment and their

procedural status. In particular, the practical methodological guidelines of the Department for Combating Cybercrime of the Ministry of Internal Affairs recommend using specialized software capable of recording screen images together with audio (such as Bandicam and similar programs) to preserve evidence of unlawful activities on the Internet, including electronic traces found on social networks and video-hosting platforms [8, p. 53]. This method is highly effective for preserving dynamic and rapidly changing information, such as live broadcasts, chats, or phishing links that may be deleted within 24 hours.

However, although the concept of "digital evidence" was introduced into the Criminal Procedure Code by Law No. ZRU-1003 adopted by the Oliy Majlis on November 21, 2024, a clear procedural mechanism for using video records and screenshots obtained through such technical software as samples for forensic examination has not yet been fully developed. In practice, a screenshot obtained by an investigator or specialist is often simply attached to the case documents as an ordinary graphic file. According to the requirements of the current O'z DSt ISO/IEC 27037:2017 state standard, however, the "non-reversibility" (non-alteration) and objectivity of every digital item of evidence or sample must be guaranteed at the time it is obtained [6, p. 12]. If the cryptographic integrity of the obtained digital sample (MD5 or SHA-256 hash code) is not recorded in the protocol, the admissibility and authenticity of such evidence may subsequently be called into question during court proceedings.

Another important aspect is that, as a result of the development of digital crime, cases of theft of funds from citizens' bank cards through phishing attacks and SIM-card remote spoofing (SIM-swap) chains are increasing [5, p. 59]. In such situations, obtaining samples from smartphones, computers, or servers related to a criminal case requires an extremely careful tactical approach. While an investigator is obtaining a sample from a technical device at the crime scene using traditional methods, there is a risk that criminals may remotely delete all traces stored in the device's memory within seconds through "cloud-based" control or specially issued commands. This, in turn, negatively affects the effectiveness of the Unified "Anti-Fraud" System introduced by President Shavkat Mirziyoyev under Resolution No. PP-155.

Therefore, in our research, we propose making it mandatory, at the time of obtaining a digital sample, to immediately technically isolate the device from external networks (by switching it to airplane mode or using special electromagnetic-shielding Faraday barriers), as well as to use "Write-blocker" devices that block the writing of information at the hardware level. These technical recommendations are not merely theoretical considerations but constitute a systematic solution aimed at directly ensuring compliance with the requirements of the applicable state standard O'z DSt ISO/IEC 27037. In addition, the methodological guidelines of the Department for Combating Cybercrime of the Ministry of Internal Affairs still prescribe the use of DVD discs as a standard form for transmitting digital data to forensic expert units [8, p. 158].

In the era of high-volume cloud data, large-scale server logs, and encrypted systems, transferring evidentiary information through such outdated storage media creates a technical risk of data corruption or insufficient storage capacity. In our research, as a solution to this problem, we emphasize the need to create a specialized online module within the "Electronic Criminal-Legal Proceedings" platform, which has been successfully implemented by the state administration, for the secure transmission of digital samples based on blockchain technology.

3. Guarantees for Ensuring Individual Rights and Freedoms

At the center of national reforms, the dignity of the individual and the protection of human rights have been identified as priority objectives. Page 19 of the O'z DSt ISO/IEC 27037:2017 standard contains an important humanitarian provision, according to which the process of collecting digital data may require a specific approach, in particular, "preservation in the presence of the data owner" [6, p. 19].

Our research has established that, when obtaining samples from digital devices or cloud servers, there is a high risk that correspondence concerning the private lives of third parties who are completely unrelated to the criminal case, as well as their family photographs or trade secrets, may also come into the possession of the investigator. In order to prevent such situations, we consider it necessary to introduce the following procedural restrictions into legislation to guarantee the constitutional rights of individuals during the investigative action of obtaining digital samples:

- strictly prohibit the inclusion in the body of evidence of electronic data containing personal or family secrets that are unrelated to the criminal case;
- formally warn specialists and experts participating in the acquisition of digital samples of their obligation not to disclose information, in accordance with the relevant provisions of the Criminal Procedure Code;
- mandatorily preserve and seal samples in

cryptographically encrypted containers in the presence of the data owner or attesting witnesses.

Such a systematic and constructive approach would be fully consistent with the policy established by the Head of State aimed at ensuring the unconditional protection of citizens' rights and freedoms in criminal proceedings and would constitute a fundamental basis for achieving this objective.

CONCLUSION

The intensive judicial and legal reforms being implemented in New Uzbekistan under the leadership of President Shavkat Mirziyoyev—including Resolution No. PP-155 (Anti-Fraud), Resolution No. PP-17 on improving the personnel training system, as well as Law No. ZRU-1003 adopted in 2024—have created a solid legal foundation for the digitalization of national criminal proceedings and the training of a new generation of specialists in this field [3; 4; 7]. Nevertheless, in the era of information technologies, the procedural and technical modernization of the investigative action of obtaining samples from digital traces for forensic examination is an objective necessity for ensuring the authenticity and admissibility of evidence in court.

Based on the results of the comprehensive research conducted by us, we put forward the following constructive recommendations aimed at further developing the field and improving the "Electronic Criminal-Legal Proceedings" system:

1. Improvement of Legislation: Supplement Article 188 of the Criminal Procedure Code with Part 5, providing for the possibility of obtaining digital samples through 3D scanning and visual modeling of objects in order to preserve their original state in the virtual environment.

2. Technical Regulation: Introduce the use of "Write-blocker" devices that prevent data modification during the acquisition of digital samples, as well as the calculation of MD5/SHA-256 hash codes, as mandatory procedural requirements in investigative and forensic practice.

3. Modernization of the "Electronic Criminal Case" System: Establish a specialized "Digital Forensic Samples Module" within the platform for the secure storage of large volumes of digital evidence and their cryptographic identifiers (hash codes), as well as for the automatic verification of their authenticity.

The implementation of these systematic solutions in practice will not only significantly increase the effectiveness of detecting cybercrimes in the immediate aftermath of their commission but will also contribute to strengthening the rule of law, standards of justice, and guarantees of human rights in our country.

REFERENCES

1. Decree No. PF-5441 of the President of the Republic of Uzbekistan dated May 14, 2018, "On Measures to Further Reform the Judicial and Legal System and Ensure the Supremacy of Legislative Acts" // National Database of Legislation (lex.uz).
2. Resolution No. PP-270 of the President of the Republic of Uzbekistan dated September 8, 2025, "On Measures to Further Improve Forensic Expert Activities" // National Database of Legislation (lex.uz).
3. Decree No. PF-6256 of the President of the Republic of Uzbekistan dated June 5, 2021, "On Measures to Further Improve Forensic Expert Activities and Strengthen Cooperation between State Forensic Examination Institutions and Non-State Forensic Examination Organizations" // National Database of Legislation (lex.uz).
4. Resolution No. PP-155 of the President of the Republic of Uzbekistan dated November 30, 2023, "On Measures to Further Improve the System for Combating Crime in the Field of Digital Technologies" // National Database of Legislation (lex.uz).
5. Law No. ZRU-1003 of the Republic of Uzbekistan dated November 21, 2024, "On Amendments and Additions to the Criminal Procedure Code of the Republic of Uzbekistan in Connection with the Improvement of the System for Handling Digital Evidence" // Collection of Legislative Acts of the Republic of Uzbekistan.
6. O'z DSt ISO/IEC 27037:2017. Information Technology. Security Techniques. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Tashkent: "Uzstandard" Agency, 2017. 70 p.
7. Resolution No. PP-17 of the President of the Republic of Uzbekistan dated January 17, 2024, "On Measures to Raise the System of Training, Retraining, and Advanced Training of Personnel for Internal Affairs Bodies to a Qualitatively New Level" // National Database of Legislation (lex.uz).
8. Methodology for Detecting Crimes Committed through Information Technologies: Methodological Guide / Cybersecurity Center of the Department of Operational-Search Activities of the Ministry of Internal Affairs of the Republic of Uzbekistan. Tashkent, 2024. 196 p.