Date: 19th January-2026

THEORETICAL AND PRACTICAL ASPECTS OF THE SEIZURE OF DIGITAL INFORMATION

Najmitdinov Nodirkhon Amrillokhonovich
Applicant to the University of Public Security of the Republic of Uzbekistan
E-mail: amrilloxon47@gmail.com

Abstract. This article examines the theoretical and practical issues associated with the seizure of digital information. Particular attention is paid to the legal principles governing seizure, including legality, proportionality, and the preservation of data integrity. The article analyzes the main challenges faced by law enforcement authorities in practice, such as technical unpreparedness, the absence of proper documentation and recording of the seizure process, the risk of data destruction, as well as the lack of clear and comprehensive legal regulation.

Key words: digital evidence, digital information, seizure, metadata, criminal process, law enforcement practice, forensic science.

In the era of rapid development of information and communication technologies, digital information has become one of the key elements of criminal proceedings. Modern criminal justice increasingly faces the need to seize, preserve, and analyze digital information [1]. Digital traces have become an integral component of the evidentiary base in the investigation of crimes ranging from fraud to terrorism. Digital information may contain evidence of criminal offenses, traces of criminal activity, as well as data of significant importance for the investigation. However, in practice, the seizure of digital information is accompanied by a number of challenges, despite the existence of theoretical foundations and regulatory legal frameworks.

According to Part 1 of Article 204¹ of the Criminal Procedure Code of the Republic of Uzbekistan, electronic data are data that are created, processed, and stored using electronic devices and information systems, as well as information technologies [2].

In theory, the procedural seizure of digital information is based on several key principles. First, the principle of legality, which means that actions related to the seizure of digital data may be carried out only by authorized bodies and strictly in accordance with the law. Second, the principle of proportionality, which requires that the scope and nature of the seized information correspond to the aims and objectives of the investigation. Third, the principle of non-interference with data after its seizure, which implies the necessity of ensuring the integrity and immutability of the information [3]. From a methodological perspective, the process of seizing digital information must be accompanied by proper documentation, including the preparation of inspection and seizure reports, the recording of the technical characteristics of devices, the condition of data carriers before and after seizure, as well as the use of specialized technical means that exclude the possibility of altering the information during the seizure process [4].

For the purposes of the present context, it should be noted that electronic data include metadata[12], the recording of which in the protocol of seizure of electronic information we consider to be mandatory.

Having regard to the distinctive characteristics of the creation, preservation and deletion of electronic (digital) data, as well as the specific features governing the collection, handling and utilization of evidence of this nature, the involvement of a qualified specialist in the examination thereof is of particular significance [5].

Specifically, in the course of examining the memory of a computing device, it was determined that an electronic document in .doc format had been created at a particular moment in time, which fact may serve to establish or exclude the existence of an alibi in respect of a given individual. Nevertheless, the specialist is entitled to state that the timestamp indicating the creation of such a .doc file is susceptible to deliberate artificial modification by any person possessing ordinary competence in the field of information technology, without encountering substantial technical obstacles.

However, the practical experience of seizing digital information reveals the existence of numerous problems that hinder the effective application of theoretical and legal norms. One of the main problems lies in the technical unpreparedness of law enforcement officers. Investigators and operational personnel often lack sufficient knowledge and skills in the field of information technologies, which leads to errors in the process of seizing digital data [6]. Such errors may result in the loss or alteration of information, violations of procedural requirements, and the recognition of digital evidence as inadmissible by the court.

As an illustrative example, a situation may be noted in which, upon the discovery of a laptop, investigators attempted to power it on. During startup, this action triggered the encryption of the data stored on the device. As a result, subsequent examination by specialists failed to unlock the device and extract the data, leading to the loss of digital information of significant importance to the investigation.

In addition, in practice there are frequent instances of excessive seizure of digital media. During investigative actions, law enforcement officers seize all accessible electronic devices, including mobile phones, tablets, and computers, belonging to relatives or other persons who have no relation to the case under investigation [7].

Another serious problem is the lack of proper documentation of the process of seizing digital information. Investigative actions are often carried out without a detailed description of the seized data carriers in the official record, without photo and video recording, and without documenting the condition of the media before and after seizure. This creates a risk of data alteration or even substitution of the data carriers themselves in

[12] **Metadata** is defined as structured information describing other information or digital objects. It comprises data about the properties, features, and context of such objects, enabling their effective automated search, classification, management, and analysis within large-scale information environments. Typical instances of metadata encompass file format, size, timestamps (creation, modification, access), authorship, device origin, and similar technical attributes.

order to conceal a crime. As a result, difficulties arise in confirming the authenticity and integrity of the obtained digital data [8].

In addition, there is the problem of the loss of operational data, which may be stored in the device's volatile memory, temporary files, caches, or cloud services. In cases of improper handling of the device, such data may be irretrievably lost, which reduces the evidentiary value of the investigation.

No less serious is the problem of the threat of information destruction by offenders. In circumstances where suspects widely use remote access tools, encryption technologies, and self-destructing files, any delay by officers in seizing digital media creates a high risk of the irreversible loss of information [9].

Moreover, the lack of appropriate technical means and insufficient legal regulation of actions in such situations create additional difficulties for the investigation. As is well known, the use of various messengers and software applications for communication is a widespread method of transmitting and receiving information among criminals, including text messages, video and audio files, images, and geolocation data. One of the most commonly used messengers today is Telegram. However, during the seizure of data carriers containing information of evidentiary value stored in the Telegram application, such data may be deleted without direct use of the mobile phone itself. Given that the Telegram application can be controlled via other connected devices, the risk of data loss constitutes one of the major problems in the collection of the evidentiary base.

In order to address the identified problems, it is necessary to adopt a set of measures aimed at improving the practice of seizing digital information. First and foremost, systematic training of law enforcement personnel is required. Investigators and operational officers should undergo specialized courses and training programs in digital forensics.

It is also necessary to develop and approve unified methodological guidelines on the procedure for seizing digital data for all law enforcement officers, taking into account both the legal and technical aspects of this procedural action.

Particular attention should be paid to the process of documenting the seizure of digital data. At the same time, it is necessary to continue efforts to improve criminal procedural legislation, in particular with regard to regulating the procedure for the seizure of information.

Thus, the seizure of digital information constitutes a complex and multifaceted process that requires maintaining a balance between the effectiveness of the investigation and the protection of citizens' rights.

In practice, a number of problems exist, related both to the technical unpreparedness of law enforcement personnel and to the absence of clear legal regulation. Only a comprehensive approach—encompassing the improvement of legislation, professional training of personnel, and the implementation of modern technologies—will make it possible to minimize the risks of loss or inadmissibility of digital evidence and to ensure the effective functioning of law enforcement authorities in the context of the digitalization of society.

REFERENCES:

1. Goodison S.E., Davis R.C., & Jackson B.A. (2015). *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence.* RAND Corporation.
2. Article 204¹. Peculiarities of collection, verification and evaluation of electronic (digital) evidence Criminal Procedure Code of the Republic of Uzbekistan (Source: http://lex.uz)
3. Kerr O.S. (2005). *Searches and Seizures in a Digital World.* Harvard Law Review, 119(2), 531–585.
4. Ahmed M., & Ko R.K.L. (2018). *Digital Evidence Management: Legal and Technical Challenges.* Computer Law & Security Review, 34(3), 550–567.
5. Rossinskaya E.R. Problems of Applying Special Knowledge in the Judicial Examination of Computer Crimes under Conditions of Digitalization // Vestnik Universiteta imeni O.E. Kutafina (Kutafin University Bulletin). 2019. No. 5 (57). P. 35.
6. Casey E. (2019). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (4th ed.).* Academic Press.
7. Ghosh S. (2022). *Overcollection of Digital Devices During Criminal Investigations: Legal Boundaries and Ethical Considerations.* Journal of Digital Law, 7(1), 10–23.
8. Solov'yev A.N. (2022). Problems of fixation and preservation of digital evidence upon their seizure // Rossiyskiy yuridicheskiy zhurnal = Russian Journal of Legal Studies. 2022. No. 1. Pp. 88–95.
9. Grishko A.V. (2021). Digital information seizure: criminalistic and legal aspects. Criminalistics and Forensic Examination, (3), 56-60.