International Journal of Law And Criminology

VOLUME Vol.06 Issue09 2026
PAGE NO. 22-27
DOI 10.37547/ijlc/Volume06Issue09-04

Some Issues in Evaluating Digital Evidence in Criminal Proceedings

Najmitdinov Nodirkhon Amrillokhonovich
Independent Researcher, University of Public Security of the Republic of Uzbekistan, Uzbekistan

Received: 28 July 2026; **Accepted:** 22 August 2026; **Published:** 15 September 2026

Abstract: This article examines the modern criteria for evaluating digital evidence based on its specific characteristics. Particular attention is given to the use of tools operating on a cryptographic algorithm to ensure the authenticity of electronic data, and the opinions of scholars on the evaluation of digital evidence are also analyzed.

Keywords: Criteria for evaluating digital evidence, metadata, relevance of evidence, admissibility, reliability, authentication, identification, verification, blockchain technology, Hash value, inadmissible evidence, screenshot.

Introduction: Today, the rapid development of information and communication technologies is fundamentally changing the methods, means, and forms of traces left by crimes. A growing portion of the traces and information generated as a result of a crime is being formed in electronic devices, information systems, telecommunication networks, social networks, messengers, cloud services, and other digital environments. In this regard, digital evidence is becoming an important tool in the process of detecting and investigating crimes, as well as proving them in court.

A distinctive feature of digital evidence is that electronic information can be easily modified, deleted, copied, or restored using technical means. Therefore, digital evidence must be evaluated not only on its content but also on the reliability of the process for its identification, acquisition, preservation, transfer, verification, and procedural formalization.

The dynamics of crimes committed using information technology underscore the relevance of this topic. According to data from the Ministry of Internal Affairs of the Republic of Uzbekistan, 863 crimes of 18 types were committed using information technology in 2019, whereas in 2024, 58,800 cases across 62 types of such crimes were registered [1]. This means that in five years, the number of crimes committed using information technology has increased nearly 68-fold. While the share of cybercrime in total crime was 6.2% in 2023, this figure reached 44.4% in 2024. In other words, in 2024, information technology was used in the commission of almost every second crime.

METHODS

This research employed methods such as empirical and systematic analysis, comparative-legal analysis, logical reasoning, modeling, and statistical data analysis.

RESULTS

According to Article 95 of the Criminal Procedure Code of the Republic of Uzbekistan, "the inquirer, investigator, prosecutor, and court shall evaluate evidence based on their inner conviction, guided by the law and legal consciousness, and grounded in a meticulous, complete, comprehensive, and objective examination of all circumstances of the case. Each piece of evidence must be evaluated in terms of its relevance, admissibility, and reliability"[2].

Based on the requirements of this article, it can be concluded that evidence presented by the inquirer, investigator, prosecutor, and court - who are the participants in the criminal procedural proof process - must meet three criteria: **1. Relevance; 2. Admissibility; and 3. Reliability.**

It should be noted that the criterion of sufficiency of evidence, as established by the legislator, is not analyzed within the scope of this study because, in our

opinion, it is subjective in nature and depends on the inner conviction of the entity evaluating the evidence.

In this regard, A.R. Belkin explains the concept of evidence evaluation as follows: "this process is an activity related, on the one hand, to processing and collecting information, and on the other hand, to forming conclusions about determining the value of the evidentiary information"[3].

Professor V.A. Lazareva puts forward another point of view, asserting that the evaluation of evidence should be understood as "a mental activity consisting of the analysis and synthesis of the content and form of the evidence"[4].

Based on the foregoing, in our opinion, the evaluation of evidence is the mental (logical) activity of an investigator (inquirer, prosecutor, or court), in which each piece of evidence is assessed in terms of its relevance, admissibility, and reliability, while the body of evidence is evaluated for its sufficiency to substantiate a specific procedural decision (including a decision on the merits of the case).

This, in turn, raises a question: can these traditional criteria also be applied when evaluating digital evidence, or is it necessary to develop new (different) criteria for them? This very question is the central issue within the scope of this dissertation research and will be answered below.

First, let us consider the criterion of relevance for digital evidence. As is well known, according to criminal procedure legislation, "evidence is recognized as relevant to the case only if it reflects information about facts or objects that confirm, refute, or cast doubt on the existing circumstances significant to the criminal case" [5].

In our view, the rules regarding the relevance of evidence in criminal proceedings can also be applied to electronic evidence. Evaluating electronic evidence from the perspective of the relevance criterion is understood as the subject of proof determining the connection between the electronic (digital) information—which constitutes the content of the digital evidence—and the circumstances that must be proven.

In this regard, we agree with the opinion of the scholar S.V. Zuyev. He emphasizes that "the relevance and reliability of digital evidence will depend entirely on its verification in the manner prescribed by law"[6]. At the same time, we believe that the evaluation criterion being analyzed should be considered a legal requirement, as failure to comply with it may lead to the inadmissibility of the evidence.

Thus, the relevance of digital evidence is understood as a legal requirement that consists of establishing a connection between electronic (digital) information and the circumstances that must be proven in a criminal case.

Moving on to the study of the admissibility of evidence as one of the evaluation criteria, we must note that this criterion has attracted particular attention from the scientific community, which is confirmed by the existence of numerous scholarly works on this topic.

The Criminal Procedure Code of the Republic of Uzbekistan states that evidence is recognized as admissible only if it has been collected in the prescribed manner and complies with the conditions stipulated in Articles 88, 90, and 92–94 of this Code [7].

As we have indicated above, regarding the criteria for the admissibility of traditional evidence, scholars A.V. Smirnov, K.B. Kalinovsky, and N.M. Kipnis have proposed the following requirements (which they also called "rules"), namely:

– the rule that evidence must be obtained from a proper source;

– the rule regarding the appropriate subject authorized to provide proof;

– the rule regarding the appropriate method of collecting evidence;

– the rule regarding the legal procedural form for collecting evidence;

– the rule regarding the legal procedure for examining evidence [8].

Based on this, we believe that any digital evidence obtained in the form prescribed by law is to be recognized as admissible evidence.

Now, the following question may be posed: in contrast to the evaluation of other types of evidence, what are the specific features of assessing the admissibility of digital evidence?

Continuing the discussion on the application of the admissibility criterion to the evaluation of digital evidence, we consider the opinion of S.V. Zuyev to be particularly noteworthy. In one of his works, the scholar puts forward the thesis that digital data should be subject to requirements such as authentication, identification, verification, and reproducibility [9].

In the following analysis, we propose to explain the essence and function of these requirements through their terminological content.

According to scholars P.P. Zaitsev, M.G. Yanin, and K.M. Kochedikova, "authentication" is understood as the ability to verify the integrity and immutability of the content of an electronic document[10].

From a criminal procedure perspective, the essence of the concept of "authentication" is as follows: the subjects of proof—the investigator or interrogator—must determine the reliability of evidence containing electronic data while conducting the preliminary investigation.

When an investigator (or interrogator) seizes a device storing electronic information or copies electronic information from it during an investigative action, they carry out the authentication process after this information is attached to the case file as evidence.

The essence of this process is that the participants conducting the proof compare the original electronic information with the subsequently obtained electronic information by its content and metadata. If they are identical, meaning they fully match in terms of content and technical characteristics, then the reliability and authenticity of the evidence is confirmed.

Based on the foregoing, we propose the mandatory application of identification and authentication processes. This, in turn, gives electronic data the quality of being verified (confirmed).

The implementation of these processes allows the participants in the proof to be clearly convinced that the electronic information is reliable and authentic. Thus, verification establishes and confirms the reliability of the evidence containing electronic information.

Recognizing the necessity of these processes allows for a deeper understanding of the unique characteristics and essence of establishing the authenticity of evidence containing electronic information.

I. In our opinion, ensuring the authenticity of information copied by a specialist or an investigator is accomplished by stating a number of defined indicators, such as: the number of copied files, their size (individually and in total), file names, and other data.

This set of defined indicators constitutes the metadata of the electronic information.

Recording this metadata in the protocol of the investigative action serves as a legal guarantee aimed at eliminating the risk of subsequent corruption or modification of the obtained information.

In our view, a cryptographic algorithm—the hash function—helps confirm the integrity and authenticity of electronic information. According to the "Guidelines for Standardization," "A hash is a hash function defined based on an agreed-upon cryptographic suite. A hash value is the bit string that is the output of the hash function" [11].

The result of processing electronic information is a checksum (hash value) in the form of a character string, which is one component of the electronic information's metadata.

If a change is made to the original electronic information, this will lead to a change (transformation) in the hash sum.

As an example, we will present a method for determining the checksum value using MD5, SHA1, and SHA256. However, these programs are not reliable, as they can sometimes generate the same checksum for different electronic files. To prevent such instances, it is recommended to use verified algorithms (SHA256, SHA512) and specialized programs—the AccessData FTK Imager and HashMyFiles utilities.

Furthermore, to ensure the integrity of electronic information, it is necessary to create an electronic "image" of it (the AccessData FTK Imager program is used for this). This image creates a complete copy of the original electronic data, and the examination is conducted on this very image—that is, the checksum is calculated and recorded in the report of the investigative action.

The checksum value allows for the identification of electronic information. The methods we have proposed make it possible to ensure the reliability of evidence containing electronic information.

We believe it is necessary to use the checksum value of electronic information in the evidentiary process within criminal procedure legislation. At the same time, special attention is being paid to the necessity of certifying the programs that determine the checksum, as this is of critical importance in ensuring the reliability of the process.

The control value of electronic information confirms its reliability. In their methodological recommendations, O.V. Khimicheva, A.V. Andreev, P.O. Panfilov, and M.Yu. Terekhov emphasize the necessity of recording this metadata element of electronic information in the protocol of an investigative action. This, in turn, serves to establish the authenticity of the evidence containing this electronic information.

These scholars have described the mechanism for determining the control value as follows: an electronic device—or more precisely, a special program—calculates a checksum of the file where the electronic information under review is stored. After the file containing the electronic information of interest is transmitted to a second device, the receiving device also determines the control value of this file. The result of the comparison is then evaluated as follows:

– if the control values on both devices match, the second device allows the user to work with this

electronic information;

– if the control values do not match, the devices automatically restart the operation.

This procedure makes it possible to prevent external interference when files containing electronic information are being transferred. Any change made to the files leads to an automatic change in the control value. To determine the checksum of files, Total Commander or the "7-Zip" archiver can be used [12].

In the protocol of the investigative action based on the results of copying, it is necessary to specify the method used to determine the checksum value (including the software used), the type (s) of the checksum, and its value. Subsequently, if the information on a web page is altered and a participant in the criminal proceedings believes this information has been falsified or modified, it will be necessary to confirm through witnesses that the content remained unchanged during the copying process. It will be possible to confirm that no changes were made to the file after its seizure by re-examining the electronic data carrier with the participation of a specialist, its subsequent interrogation, and by recalculating the same type of checksum. Furthermore, when seizing an electronic data carrier or a portion of its data by copying, it is always advisable to determine the checksum of the file.

II. Identification of Electronic Information — is a process that allows for the reliable confirmation, based on a digital object's individual characteristics, that it originated from a specific source and has not undergone any modifications.

In other words, identification is the process of determining the exact source to which the provided data (files, messages, information, etc.) belongs and that it has been preserved in an unaltered state.

In practice, any digital evidence (e.g., an email, video recording, chat correspondence, server logs, etc.) is considered to have evidentiary value only if the following conditions are met:

- the author of the information must be identified;
- the authenticity (that it has not been altered) of the information must be ensured;
- the integrity (that it has not been partially deleted or falsified) of the information must be confirmed;
- the information's link to a specific device or account must be proven.

In this regard, the identification process establishes the technical uniformity (correspondence) of the evidence, determining that it originates from a reliable and verified source.

The following methods and tools are used to identify electronic information:

- Hash functions (SHA-256, MD5, etc.): to verify that the data has not been changed;
- Metadata: to identify the source through the information's creation time, IP address, device number, and more;
- Unique device identifiers (IMEI, MAC address, serial numbers) ;
- Digital signatures and electronic certificates;
- System log files, i.e., user login history, internet activity, network connections, etc.

These tools not only help find information but also directly serve to establish its source and authenticity. When evaluating digital evidence, identification is considered a criterion for reliability. If an expert or investigator cannot prove the source and origin of the information, such evidence may be deemed inadmissible by the court in accordance with Article 951, Part 1, Clause 5 of the Criminal Procedure Code of the Republic of Uzbekistan (from an unknown source or from a source that could not be identified during the criminal proceedings) .

Identification methods are particularly important in the investigation of terrorism-related crimes. For example: determining whether a file found on a terrorist group member's phone was created on that specific device and has not been altered; establishing the true source of an encrypted message or "chat" data; and confirming that the metadata of electronic information (date, GPS coordinates, etc.) corroborates the actions of the person suspected of committing the crime.

In these cases, identification confirms the authenticity of electronic evidence, allowing it to be accepted as reliable evidence in a criminal case.

III. In turn, the concept of verifiability in relation to electronic (digital) information can be defined as follows: it is the actions of a person authorized to evaluate evidence, aimed at processing and analyzing this information, with the purpose of verifying its reliability.

Based on the requirements stipulated in Article 2042 of the Criminal Procedure Code, verifying the authenticity of an evidentiary source containing electronic information is the process of determining that no alterations have been made by analyzing the data on the electronic storage medium. Thus, evidential value is attributed only to electronic information that has undergone identification and authentication, meaning such information acquires the status of verified

electronic information.

IV. As noted by the scholar S.V. Zuyev, the reproducibility of information (vosproizvodimost svedeniy) refers to the ability to display it in a simple and understandable manner. Indeed, when it comes to the reproducibility of electronic (digital) information, ensuring its displayability is crucial, which can only be accomplished using special software and hardware. In our opinion, these requirements defined by S.V. Zuyev are fully applicable to the processes of verifying and evaluating electronic evidence; the main thing is to implement them consistently.

An analysis of the content of the admissibility criterion for digital evidence in modern criminal procedure, particularly the study of what requirements criminal procedural evidence must meet, allows us to formulate the content of this evaluative criterion.

Thus, the criterion for the admissibility of digital evidence is a legal requirement which stipulates that digital evidence obtained during the investigation of a criminal case must comply with the following: it must be procured by the appropriate subject of proof; the evidentiary information must be obtained from a relevant source; the method and form of collecting the evidence, as stipulated in the Criminal Procedure Code of the Republic of Uzbekistan, and the procedures for verifying evidence must be adhered to; and the authentication, identification, verification, and reproducibility of the electronic information must be ensured.

The proposed definition clarifies the meaning of the admissibility criterion for digital evidence, defining its specific characteristics and the aspects to which a person authorized to evaluate evidence must pay close attention. This point is particularly relevant because there have been cases in practice where digital evidence was deemed inadmissible in a criminal case.

According to Article 95 of the Criminal Procedure Code of the Republic of Uzbekistan, "Evidence that is determined to be true as a result of verification shall be considered reliable."

Reliability is one of the key criteria for evaluating evidence, holding significant importance alongside relevance and admissibility. However, as a general rule, this criterion is usually applied during the final stage of the proof-gathering process.

In the explanatory dictionary of the Uzbek language, "ishonchli" (reliable) is defined as trustworthy or unfailing [13].

At the beginning of this article, we will focus on the relationship between admissibility and reliability as criteria for evaluating evidence. It is crucial to understand the distinction between them, as it is expressed as follows: "The admissibility of evidence is evaluated based on the criteria established by law, whereas reliability is evaluated based on the content of the evidence".

In this regard, the views of A.A. Kupriyanov on information systems based on blockchain principles are noteworthy. According to the author, such a system guarantees the complete immutability of information recorded in any block ledger. Therefore, "information stored using blockchain technology can undoubtedly be recognized as evidence in criminal proceedings, as it allows for the identification of the time the information was recorded, its transmission, its receipt by the addressee, as well as the sender and the recipient". At the same time, the scholar notes that verifying the reliability of data in a blockchain system is easily accomplished.

Based on the foregoing, we propose to define the algorithm (or rules) for determining the reliability of electronic information as follows:

1. Determining the technical condition of the electronic data carrier (whether it is in working order; whether the electronic data stored on it is accessible, etc.), as well as establishing its characteristics and technical specifications (e.g., whether it is designed for storing, processing, or transmitting electronic data, etc.). This procedure makes it possible to determine its functional capabilities.

2. Identifying the owner of the electronic data carrier (to the extent possible) and the person who created the electronic data stored on it, i.e., its author.

This action makes it possible to determine whether there was a vested interest in altering the electronic data. This, in turn, is determined based on information available to pre-investigation or judicial authorities, taking into account the personal characteristics of the electronic data carrier's owner and the person who created the electronic data.

3. Analyzing the content of the electronic data, including an examination of the circumstances of its creation.

In carrying out this action, the main focus should be on identifying potential contradictions within the provided data, as such inconsistencies can be indicators of the electronic data's reliability or authenticity. If such contradictions are found, they must be critically compared with other evidence available in the criminal case during their evaluation.

Thus, the presented algorithm for determining the reliability of electronic information should be recognized as universal, yet not exhaustive. This is

because, depending on the specific circumstances of the case, the entity assessing the evidence may also perform other actions aimed at establishing the authenticity of the information in electronic form.

At the same time, according to the researcher, it is advisable to use the following universal formula to determine the reliability of evidence: "Evidence is recognized as reliable if no doubt remains as to its authenticity" (beyond a reasonable doubt). This formula can be applied from the perspective of the reliability criterion when evaluating digital evidence.

CONCLUSION

In our opinion, the scientific community and legislative bodies should take a thorough approach to the issue of clearly defining the rules for evaluating evidence (in particular, digital evidence) from the perspective of the reliability criterion. This is relevant not only in administrative proceedings but also in criminal proceedings. Furthermore, these rules must be enshrined in the norms of the relevant codes. This is, above all, crucial for forming a unified judicial and investigative practice regarding the use of digital evidence.

The results of the conducted research show that the rapid development of digital technologies is fundamentally changing not only the methods of committing crimes but also the mechanisms for their investigation and criminal procedural proof. Unlike traditional evidence, the volume, variety, rapid mutability, and technical characteristics of electronic data generated in the digital environment require a special procedural and forensic approach to its evaluation. From this perspective, the issue of evaluating digital evidence is inextricably linked not only to determining its content but also to a comprehensive examination of its source, mechanism of creation, integrity, authenticity, the legality of the method of acquisition, and procedural documentation.

The analysis conducted within the scope of the study showed that while the general criteria applied to traditional evidence retain their significance in evaluating digital evidence, it is also necessary to introduce additional criteria stemming from the unique characteristics of digital data. Specifically, in addition to the relevance, admissibility, and reliability of digital evidence, its authentication, integrity, accuracy of the source of origin, preservation of the digital footprint, and continuity of the chain of custody must be evaluated separately. The comprehensive application of these criteria enables judicial and investigative authorities to determine the true evidentiary value of digital information.

REFERENCES

1. Number of crimes listed – SIAT. // http://stat.uz
2. Article 95 of the Criminal Procedure Code of the Republic of Uzbekistan // http://lex.uz
3. Belkin A. R. Theory of Evidence in Criminal Proceedings: in 2 parts. Part 1: a textbook for universities. 2nd ed., revised and supplemented. Moscow, 2021. P. 65.
4. Lazareva V. A. Evidence in Criminal Proceedings: a textbook for universities. 7th ed., revised and expanded. Moscow, 2021. P. 51.
5. Article 95 of the Criminal Procedure Code of the Republic of Uzbekistan // http://lex.uz
6. Zuev S. V. Electronic Evidence in Criminal Proceedings: Concept and Significance // Law and Order: History, Theory, Practice. 2020. No. 3 (26). P. 49.
7. Article 95 of the Criminal Procedure Code of the Republic of Uzbekistan // http://lex.uz
8. Smirnov A. V., K. B. Kalinovsky K. B. Criminal Procedure: a textbook / edited by Prof. A. V. Smirnov. 4th ed., revised and supplemented. Moscow, 2008. Pp. 186–190.
9. Zuev S. V. On the Modern Concept of the Development of Information Technologies in Criminal Proceedings (RITVUS) // Perm Legal Almanac. 2019. No. 2. P. 621.
10. Zaitsev P. P. Electronic Document as a Source of Evidence // Legality. 2002. No. 4. Pp. 43–44; Yanin M. G., Kochedykova K. M. Problems of Collecting, Verifying, and Assessing Electronic Evidence in Criminal Proceedings // Management in Modern Systems No. 2 (22). 2019. Pp. 28–31. P. 29.
11. O‘z DSt ISO/IEC 27037:2017 “Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence” (Date of introduction: 14.11.2017) T.2017.
12. Khimicheva O. V., Andreev A. V., Terekhov M. Yu., Panfilov P. O. Methodological recommendations “Procedural procedure for the use of information technologies in collecting traces of crimes and their use in proof.” 2022. Pp. 66–68.
13. A.Under Madvaliev Ed. Explanatory Dictionary of the Uzbek language. – B. 258. // https://n.ziyouz.com/books/uzbek_tilining_izohli_lugati.
14. Kupriyanov A. A. Blokcheyn-eto dokazatelstvo // Ugolovny prosess. 2022. № 1. S. 9.