The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 144-152
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-21

IMPACT FACTOR
2021: 5. 952

Admissibility Of Electronic Evidence In Criminal Proceedings

Khosiyat Mamatkulova
Teacher At The Department Of Criminal Procedural Law Of Tashkent State University Of Law, Uzbekistan

ABSTRACT

This article attempts to analyze the institution of admissibility of evidence, in particular electronic evidence. Some issues of the specifics of such evidence are also considered. As a result, some recommendations were developed to ensure the issue of admissibility of electronic evidence.

KEYWORDS

Evidence, properties of evidence, electronic evidence, admissibility of electronic evidence, criminal procedure.

INTRODUCTION

The issue of admissibility of evidence is one of the central issues in the process of proving. So, according to the article 94 of the Criminal Procedure Code of the Republic of Uzbekistan, the decision on the case can only be based on evidence subjected to thorough, complete, comprehensive and objective verification [10]. Verification consists in collecting additional evidence, which can be confirmed or refuted verifiable evidence.

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 144-152
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-21

IMPACT FACTOR
2021: 5. 952

Verification of evidence can be carried out by comparing them, analyzing, establishing the source of evidence, as well as through the production of investigative and other procedural actions, during which new evidence is obtained, which are then compared with the evidence being verified.

During the check, the properties of evidence and the source of their origin are investigated, the reliability of the information contained in the evidence is established.

Difficulties in verifying electronic evidence are determined by the specifics of digital information. Electronic media often contain a huge number of files, and the information necessary for use in the process of proof can be hidden or destroyed, as a result of which special software is required to detect or restore such information.

The next feature of checking electronic evidence is the need to seek the help of a specialist in the course of working with such evidence. Asking the right questions to the professional is an important part of the electronic evidence verification process [12, p. 502].

Verification of the source of electronic evidence assumes that the originals of electronic media must be preserved, which will help establish that no modifications have been made by technical means.

With respect to the information contained in an electronic document, as indicated by some authors [3, p. 43], there must be a possibility of its identification and authentication, which are a prerequisite for checking such a property of evidence as its reliability. In this case, authentication should be understood as the ability to verify the integrity and invariability of the content of an electronic document, and identification - the ability to identify the person from whom such a document was received [3, p. 44]. If necessary, expert opinions must be submitted confirming that no changes have been made to electronic documents. In some works, it is proposed to carry out step-by-step documentation of the identification properties of a file when doing any actions with it, in particular, when moving [1, p. 82].

The verification of evidence is the next element of the proof process in criminal proceedings. All elements of evidence, as noted above, are closely interrelated, so the verification of evidence cannot be artificially separated from the collection and assessment.

To check means to make sure something is correct, or to test something to find out. "Check" - "establish the correctness, accuracy" of something, or "do" something "in order to find out the properties, quality" of something. "Accordingly, the check referred to in Article 94 of the Criminal Procedure Code of the Republic of Uzbekistan, - this is a specific, both a mental and logical, and other kind of process carried out in order to establish the reliability or unreliability of both part of the information constituting the proof, and the entire content of the evidence as a whole.

Verification begins from the very beginning of the proof and continues throughout the preliminary investigation, judicial investigation and subsequent stages of criminal proceedings. The verification of evidence at various stages of criminal proceedings has its own characteristics. At the initial stage of the investigation, this procedure seems to be

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 144-152
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-21

IMPACT FACTOR
2021: 5. 952

quite complicated, since by this time only isolated facts have been established that indicate signs of a crime, and the participants in the inspection (interrogator, investigator, prosecutor) still do not have a complete idea of the crime committed. In this case, the verification, which began during the formation of evidence, continues for a considerable time, sometimes up to the end of the preliminary investigation. The establishment of the truth at this stage also occurs in conditions of limiting the action of a number of principles of the criminal process, namely: transparency, immediacy, competition and equality of the parties. At this stage, the content and results of the investigation of evidence may be influenced by the prosecutor, the head of the inquiry body, the head of the investigative department, the head of the investigative body [11, p. 38].

The purpose of proof is not a probable, but a reliable establishment of the circumstances included in the subject of proof, for which it is necessary to collect, verify and evaluate such a set (system) of evidence, which would be sufficient to establish each element of the subject of proof. The purpose of checking evidence in theory is interpreted by most authors as understanding the qualities and properties of the evidence being checked - their reliability or unreliability, correctness or incorrectness, good quality. Yu.V. Khudyakova notes that the above interpretation of the purpose of checking evidence does not fully characterize this complex process. In her opinion, such an important moment as the search, accumulation of knowledge about the properties, connections and relationships of the circumstances established by this evidence is excluded from the verification of evidence. The purpose of checking evidence expresses a complex phenomenon that refers not only to the sphere of thinking of the investigator, interrogator, court, but also to the practice of collecting evidence.

"Thus, the purpose of the verification of evidence is a comprehensive and complete understanding of the qualities and properties of the evidence itself, as well as the search, accumulation and analysis of knowledge about the properties, connections and relationships of actions and events established by this evidence with the evidence itself." We support this point of view. However, in this definition, I would like to concretize that under a full understanding of the qualities and properties of evidence is verification of their reliability, that is, compliance or inconsistency of the information contained in them with facts and circumstances that are important for the correct resolution of a criminal case, as well as mandatory verification of the admissibility of evidence for compliance of their form with the legal requirement of admissibility.

Verification is the most difficult element for computer information. Its complexity lies in the fact that on non-volatile storage media, so-called external media (hard drives and all kinds of removable media), the number of files is measured in tens of thousands, these are system files, program files, data files. The required information can be hidden, encrypted or deliberately destroyed.

In this case, when checking (researching), the search, accumulation and analysis of computer information is carried out, its connections with the event under investigation are determined. To recover deleted information, or decryption, special software is used, for example, a software and

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 144-152
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-21

IMPACT FACTOR
2021: 5. 952

hardware tool for forensic research of computer storage media "EnCaseForensis Edition". This software must meet the criterion based on scientific knowledge, this criterion is met if the software product used has been certified and the activity for its creation is licensed.

Verification of computer information is a complex and time consuming element. The difficulty lies in the fact that on non-volatile storage media, so-called external media (hard drives and all kinds of removable media), the number of files is measured in tens of thousands, these are system files, program files, data files.

The necessary information can be hidden, encrypted or erased (intentionally destroyed). In this case, when checking (researching), the search, accumulation and analysis of computer information is carried out, its connections with the event under investigation are determined. To recover deleted information or decrypt, special software is used. This software must meet the criteria based on scientific knowledge, that is, it must be a certified software product.

The purpose of the verification of evidence is a comprehensive and complete understanding of the qualities and properties of the evidence being verified, that is, the correspondence or inconsistency of the information contained in them with the facts and circumstances that are important for the correct resolution of the criminal case. To perform these tasks, it is necessary to comply with the following rules, to establish the technical means (hardware) from which this information was obtained or copied and its material carrier, as well as to establish the correspondence of the type, type of material carrier of computer information with the one indicated in the protocol of the investigative action, the conclusion of a specialist, expert opinion; the installation of the software with which this information was obtained.

It is necessary to highlight two aspects, firstly, what software tool was used to generate this information, for example, the creation of recording event logs occurs through the operation of the operating system, and secondly, what software tool was used for copying if this information was copied to removable media or in a separate file.

Indicating the characteristics of software tools in the protocol of an investigative action, for example, it is necessary to indicate the type of operating system, registration number, setting the details of computer information, such as the type of file, its size, creation time, editing time, opening time, user information (for data files created by application programs, information about the user is stored), establishing how the condition of data integrity (invariability) is ensured, indicate in the protocol of the investigative action which software tools are used to ensure data integrity.

To perform the task of preserving the integrity of computer information, in our opinion, it is possible to use the hashing principle, which is widely used in various programs, for example, md5sum, as well as an electronic digital signature.

Article 95 of the Code of Criminal Procedure of the Republic of Uzbekistan [10] establishes an inquiry officer, investigator, prosecutor and court to evaluate evidence according to their inner conviction, based on a thorough, comprehensive, complete and objective study

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 144-152
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-21

IMPACT FACTOR
2021: 5. 952

of all the circumstances of the case, guided by law and legal awareness. Each of the evidence is subject to assessment in terms of relevance, admissibility and reliability.

Evidence is deemed to be relevant to a criminal case if it represents information about facts or objects that confirm, refute or cast doubt on the conclusions about the existence of circumstances relevant to the case.

Evidence is recognized as reliable if, as a result of verification, it turns out that it corresponds to reality.

The totality of evidence shall be deemed sufficient to resolve the case if all reliable relevant evidence has been collected that undeniably establishes the truth about each and every circumstance subject to proving.

The common grounds for evaluating evidence are inner conviction, conscience, and the law. Special grounds for evaluating computer information as evidence are psychological, epistemological, and legal. When evaluating computer information, it is necessary to proceed from the characteristics of this type of evidence and take into account that this type of evidence consists of several elements. The task of the subjects of the assessment is to trace the entire path of the formation of computer information as a result of the reflection of a fragment of the event of a crime or the circumstances of the commission of a crime before the appearance of this computer information in the case.

One of the properties of evidence is their relevance, which is a requirement addressed to the content of the evidence, this is the ability of the evidence to serve as a means of establishing the circumstances that are important for a particular case by its content [6, p. 40; 9, p. 73].

As noted by N.A. Zigura and A.V. Kudryavtseva, "the peculiarity of determining the relevance of computer information is that it is possible when reproducing this information using technical means and analyzing not only the content of computer information, but also its properties (details). From the point of view of relevance, both the content of computer information and its properties are assessed: the date of creation, change, discovery "[4, p. 125]. At the same time, establishing a connection between electronic evidence and circumstances relevant to a criminal case often requires the participation of a specialist or an examination.

Admissibility reflects a requirement for the form of evidence. This property indicates the need to comply with the formal requirements provided by law.

In its most general form, we formulated the admissibility requirement from the following elements:

1. The legality of the source;
2. The legality of the circumstances of the formation of evidence, the method of obtaining it;
3. Proper procedural registration of evidence;
4. A proper subject, authorized to carry out actions to obtain evidence [6, p. 143].

We will not consider the general requirements for the admissibility of evidence in relation to digital information (and in particular - to electronic documents), however, we draw attention to the fact that in order to recognize objects of digital information as admissible evidence in a case, taking into account the

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 144-152
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-21

IMPACT FACTOR
2021: 5. 952

specifics of such objects, it is important to comply with the condition that information on the medium remains unchanged. which can be achieved through the use of special software [4, p. 128].

Some scientists call the properties of the relevance and admissibility of evidence a guarantee of their reliability.

As criteria for the reliability of electronic evidence, N.A. Zigura and A.V. Kudryavtsev is distinguished by the following:

First, such evidence must be generated as a result of the correct operation of the hardware and software.

Secondly, the question of the scientific nature of methods for obtaining digital information should be resolved, which is especially important in the case of obtaining such information using special software.

Thirdly, it is necessary to resolve the issue of ensuring the immutability of digital information.

And finally, the reliability of digital information must be confirmed by analyzing its content and properties and comparing it with other evidence.

At the same time, the authors note that the assessment of electronic evidence from the standpoint of reliability requires attention "both to the correctness of the data and to the correct functioning of the processing program" [4, p. 131].

Doubts about the reliability of electronic documents are determined, in particular, by the fact that it is easy to make changes to such documents, which will be difficult to detect without the help of an expert. As noted in their article, A.S. Alexandrov and S.I. Kuvychkov, "one of the modern protection strategies is to undermine confidence in electronic information presented as evidence" [1, p. 77]. However, any fact of working with a file, including various modifications of digital information, can be established and verified with the help of an examination.

Let us turn to the last property of evidence, which characterizes their totality in terms of "persuasiveness to substantiate any conclusion or procedural decision" [4, p. 132].

As noted by N.A. Zigura and V.A. Kudryavtseva, when determining sufficiency as a property of evidence in relation to digital information, there is no need to collect all the information available on the investigated electronic medium. Nevertheless, often when appointing a computer-technical examination, investigators and judges incorrectly formulate questions before experts: in some cases, for example, you may encounter a requirement to restore all deleted files, and with such a question, this requirement cannot be fulfilled due to the fact that there are a huge number of copies of files.

So, any left traces are created, transmitted, stored and read only through the use of information technology or programs. From which it follows that the environment in which these traces are stored is not familiar to human perception. Regarding traces that do not have the properties of direct perception, V.Ya. Dorokhov writes that in this case, the main qualities of the signal are lost (to be a carrier of information), and the information contained in them is not included in the field of view of the investigation authorities and the court. In this regard, special technical means or software are needed to reproduce

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 144-152
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-21

IMPACT FACTOR
2021: 5. 952

the discovered traces and their recognition as evidence. Discovered traces, which are reproduced with the help of special devices or programs, in fact, cannot be recognized as evidence until their proper procedural registration [2].

Evidence is collected through the production of investigative and judicial actions. Unfortunately, when investigating crimes in the field of information technology, the abundance of procedural actions loses all meaning, since all attempts are reduced to one thing - inspection. Many process scholars adhere to this position.

The information and objects obtained as a result of the inspection can be used as evidence only after they have been recorded in the relevant protocols. The procedure for drawing up a protocol of investigative actions is aimed at ensuring the completeness and reliability of the reflection in a criminal case of the course and results of investigative actions in accordance with the specifics of each of their types and the specific conditions of production [8].

According to V.A. Meshcheryakova, V.V. Trukhachev, in a generalized form, the mentioned complex of requirements, which makes it possible to talk about the possibility of forming electronic digital objects of evidence from the detected (sought) objects, looks as follows [5]:

The correctness of fixing the main events (the formation of the necessary electronic digital object) in the computer system under study (correctly set system time of the computer system, properly correctly configured procedure for recording the required set of events in the system logs);

The correctness of the transfer of the required electronic digital objects to the storage / archiving place;

Correct processing of the sought electronic digital objects in the receiving computer system;

The immutability of the storage of the required electronic digital objects until the moment of their discovery;

The correctness of the copying procedure for the desired electronic digital objects;

The immutability of the storage of the desired electronic digital objects after copying until their corresponding research;

The correctness of the interpretation of the connection of the sought electronic digital objects with the crime event.

In addition, it is necessary to note the Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan "On some issues of the application of the norms of the criminal procedure law on the admissibility of evidence" dated August 24, 2018 [7]. According to paragraph 2 of this Resolution, the conditions for the admissibility of evidence are as follows:

The evidence must be obtained by the proper subject, that is, by a person entitled to carry out the procedural action in the course of which the evidence was obtained;

Factual data should be obtained only from the sources listed in the second part of Article 81 of the CPC;

Evidence must be obtained in compliance with the rules and procedure for conducting the procedural action, during which the evidence was obtained;

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 144-152
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-21

IMPACT FACTOR
2021: 5. 952

Upon receipt of evidence, all requirements of the law on recording the course and results of the investigative and judicial action must be observed.

Evidence, in particular, is recognized as inadmissible if the evidence was obtained in an illegal way, that is, without observing the procedural rules for their collection provided by law.

Also, in accordance with article 951 of the Criminal Procedure Code of the Republic of Uzbekistan [10], factual data are recognized as inadmissible as evidence if they are obtained by illegal methods or by depriving or restricting the rights of participants in criminal proceedings guaranteed by law or in violation of the requirements of the code, including those obtained:

1) with the use of torture and other cruel, inhuman or degrading treatment and punishment in relation to participants in criminal proceedings or their close relatives;
2) by their falsification (counterfeiting);
3) with violation of the rights of the suspect, accused or defendant to defense, as well as the right to use the services of an interpreter;
4) as a result of a procedural action in a criminal case by a person who does not have the right to carry out proceedings in this criminal case;
5) from an unknown source or from a source that cannot be established in the course of criminal proceedings;
6) from the testimony of the victim, witness, suspect, accused, defendant during the interrogation, preliminary investigation, which did not find their confirmation in court by the totality of the available evidence.

Summarizing what has been said, it should be noted that the verification and assessment of electronic evidence, on the one hand, is subject to both general laws inherent in the verification and assessment of evidence in criminal cases. On the other hand, due to the specifics of digital information objects, verification and evaluation of electronic evidence requires the use of special knowledge about the nature of this kind of information, as well as, where necessary, the use of appropriate software and hardware.

In addition, the investigator must have the appropriate knowledge in the field of informatics at least an entry level, since any careless access to this kind of information can lead to the loss of its evidentiary value.

REFERENCES

1. Alexandrov A.S., Kuvychkov S.I. On the reliability of "electronic evidence" in criminal proceedings // Criminalist Library: scientific journal. No. 5 (10). M., 2013.- p. 76-84.
2. Bogdan Sh, Rasulev A, Sobirov Sh. How the collection of cyberworms is carried out. // Information Security" No. 1, 2017. - p. 36-38.
3. Zaitsev P. Electronic document as a source of evidence // Legality. 2002. No. 4.
4. Zigura N.A., Kudryavtseva A.V. Computer information as a type of evidence in the criminal process of Russia: monograph. M., 2011 .- 176 p.
5. Meshcheryakov V.A., Trukhachev V.V. Formation of evidence based on

electronic digital information // Bulletin of the VI Ministry of Internal Affairs of Russia. - 2012. - No. 2.

6. Orlov Yu.K. Fundamentals of the theory of evidence in criminal proceedings: scientific-practical. allowance. M., 2000 .- 138 p.
7. Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan "On some issues of the application of the norms of the criminal procedure law on the admissibility of evidence" dated August 24, 2018 No. // https://lex.uz/docs/3896598
8. Pyanzina E.V. Assessment of evidence from the point of view of the proper procedure for carrying out and registration of investigative actions // Bulletin of SUSU. Series: Right. - 2012. - No. 20 (279).
9. Criminal procedure: textbook for undergraduate law schools / ed. O.I. Andreeva, A.D. Nazarova, N.G. Stoyko, A.G. Tuzova., 2014 .- 445 p.
10. Criminal Procedure Code of the Republic of Uzbekistan // https://lex.uz/docs/111463#186560
11. Uralovna M. K. Subjects of proof in criminal procedure on the legislation of the Republic of Uzbekistan //European science. – 2020. – №. 1 (50).
12. Mamatkulova K. Concept And Types Of Computer Information As Evidence In The Criminal Process Of The Republic Of Uzbekistan //The American Journal of Social Science and Education Innovations. – 2020, №. 08. – p. 501-506.