Date: 17th January-2026

SOME PARTICULARITIES OF THE PROCEDURAL SEIZURE OF CARRIERS OF ELECTRONIC (DIGITAL) INFORMATION

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

Abstract. The paper demonstrates that the modern understanding of the procedural seizure of electronic data carriers must take into account not only the formal requirements of criminal procedural law, but also the technical realities of the digital environment, including the high vulnerability of data to manipulation and the necessity of applying internationally recognized standards, primarily ISO/IEC 27037. The article is intended for investigators, inquiry officers, judges, defense attorneys, as well as specialists in the field of computer and technical forensics and digital forensics.

Key words: digital evidence, electronic information, seizure, ISO/IEC 27037, metadata, identification, acquisition, preservation, evidence inadmissible, forensic science.

In the context of the digitalization of social relations and the active integration of information and communication technologies into everyday life, electronic information and its carriers acquire particular significance in contemporary criminal proceedings. Computers, mobile devices, servers, cloud storage systems and other carriers of electronic information are increasingly becoming key sources of evidence in criminal cases, reflecting facts, circumstances and traces of criminal activity. In this connection, the procedural seizure of carriers of electronic information assumes not merely practical, but also fundamental legal importance.

Modern investigative practice demonstrates that the effectiveness of crime detection and proof largely depends on the correctness and lawfulness of actions performed at the initial stage of working with electronic carriers. Failure to comply with the requirements established by criminal procedure legislation during their seizure may result in the loss of valuable data, distortion of information, infringement of the rights of participants in the proceedings, and recognition by the court of the obtained digital evidence as inadmissible. Thus, the issues of procedural formalization and actual implementation of the seizure of electronic carriers are directly linked to ensuring the principles of legality, admissibility and reliability of evidence.

The rules for the collection of digital evidence (digital/electronic evidence) in criminal proceedings are aimed at ensuring its admissibility, reliability, integrity, and authenticity in court. The collection process must be carried out in compliance with the principles of minimal interference, proper documentation, and protection against alteration.

Article 205 of the Criminal Procedure Code of the Republic of Uzbekistan specifies the methods for obtaining digital evidence. In particular, electronic data and other records used as digital evidence may be obtained during the inspection of the scene of the incident

or other areas and premises, as well as from technical devices, telecommunication networks, or the global information network Internet, in the course of seizure and search procedures [1].

The international standard ISO/IEC 27037:2012 (*Guidelines for identification, collection, acquisition and preservation of digital evidence*) establishes four key phases in the collection of digital evidence:

- **Identification** — identification of potential sources of digital data (devices, storage media, cloud services, logs, RAM, etc.).
- **Collection** — collection without altering the original data (use of write blockers when connecting storage media, photographing the seizure location, recording the condition of the device).
- **Acquisition** — creation of an exact bit-by-bit copy (forensic imaging) using specialized software (FTK Imager, EnCase, dd, Autopsy, etc.).
- **Preservation** — ensuring the preservation of the original and copies by recording hash values (preferably SHA-256) and maintaining the chain of custody[8] [2].

Key principles (mandatory in most jurisdictions):

- Work only with copies; the original must not be altered.
- Immediately calculate and record control hash values.
- Maintain a complete chain of custody, documenting who accessed the evidence, when, where, and for what purpose.
- Photograph and/or video record the device at the moment of discovery (screen, cables, surrounding environment).
- Use anti-static packaging and avoid exposure to magnetic fields and extreme temperatures.
- Involve a specialist (expert) at the collection stage, especially when dealing with volatile data (RAM, network connections).

The rules for the collection of digital evidence (digital/electronic evidence) in criminal proceedings are aimed at ensuring its admissibility, reliability, integrity, and authenticity in court. The collection process must be carried out in compliance with the principles of minimal interference, proper documentation, and protection against alteration [3].

Based on the analysis of literature related to digital forensics, when seizing and examining an electronic object, we recommend—initially with the involvement of a specialist—the following algorithm of actions:

1. Attention should be paid to whether electronic devices are powered on or turned off. Devices connected to the global Internet network should be switched to

[8] The **chain of custody** demonstrates to the court that the digital evidence presented in the courtroom is the same evidence that was seized at the scene of the incident and that it was not altered at any stage of handling. In most jurisdictions (including the United States, the United Kingdom, EU countries, Russia, and Uzbekistan), a breach of the chain of custody constitutes one of the primary grounds for declaring digital evidence inadmissible.

"airplane mode" in order to prevent remote access and external interference with the data stored in the device's memory.

2. During the seizure of electronic devices, special attention must be given to whether the device is connected to a power supply. Seizing a device by directly disconnecting it from the power source may result in the loss of data stored in volatile memory (RAM) and may also cause damage to the remaining data on the hard drive. For this reason, a specialist should use dedicated forensic software, such as Belkasoft Live RAM Capturer, CaptureGUARD Gateway, or the Volatility Framework, to create a memory dump of the device's random-access memory, thereby enabling subsequent analysis.

This is because, in the case of an electronic device that remains powered on, the volatile memory may contain the following information of evidentiary value:

2.1. Data relating to the user's current activity, including open documents and files such as text documents, images, PDF files, and other file types; as well as clipboard data, including copied passwords and messages. By way of example, this may include login credentials and passwords for accessing bank accounts.

2.2. Information on active network connections, including IP addresses, ports, web pages, and connections to anonymization networks such as VPN or Tor.

2.3. Data relating to encryption keys and session tokens, including temporarily generated encryption keys for accessing files or applications, as well as session tokens used to connect to online services (messengers, email services).

2.4. Information concerning unencrypted passwords, for example, passwords entered to open ZIP archives in applications such as WinRAR.

2.5. Information relating to messages in messengers. Where an active session exists, records obtained from messengers such as Signal, Telegram, and WhatsApp may be accessed, for example, discussions of criminal plans or exchanges of confidential information.

2.6. Browser data, including open tabs, visited web pages, and form data (logins and passwords).

2.7. Information on cached media files. Images, videos, and audio files may be temporarily stored in random-access memory even if they have been deleted from the disk. By way of example, this may include instructional videos related to the manufacture of explosive substances.

In the random-access memory of smartphones operating on the Android and iOS operating systems, data such as messages from social networks and applications, logs of GPS activity and background processes, Face ID and fingerprint identification data, as well as cached images and videos recently captured via the camera, may be stored.

3. During the seizure of electronic devices and the examination of their memory, physical copies of electronic data should be created using auxiliary tools and software without compromising the integrity of the data.

3.1. During the examination of mobile devices, attention should be paid to the following information, which must be documented through photo and video recording and reflected in the official report: IMEI numbers; recently used applications and programs (stored in RAM); SMS messages (search by keywords; review of archived, spam, and deleted messages); incoming and outgoing call history; browser windows opened and browsing/search history; media files stored, deleted, or hidden in file manager applications (audio, photo, and video files); data from social networks and messengers (accounts, connected active devices, stored messages, deleted and blocked accounts, account names entered in search fields, users with whom chats exist, groups and channels joined); data of synchronized accounts accessed via the settings application (logins, passwords, etc.); applications of payment service providers and cryptocurrency exchanges installed on the device (active sessions, personal profile data, linked accounts, and transaction history); notes recorded in reminder applications; and addresses and coordinates searched via navigation applications. It is also advisable to attach screenshots and photographs to the report in chronological order in the form of a photo table.

3.2. During the examination of personal computers, the following information should be examined: serial numbers and markings on the system unit or laptop casing; software loaded and data stored in RAM and the clipboard; email correspondence (keyword searches; review of archived, spam, and deleted messages); browser windows opened, visited pages, and browsing/search history; media files stored, deleted, or hidden in file manager applications (audio, photo, and video files); data from social networks and messengers, as well as from restricted-access websites (accounts, connected active devices, stored messages, deleted and blocked accounts, account names entered in search fields, users with whom chats exist, groups and channels joined); browser settings or credentials (logins and passwords) for cloud storage technologies such as iCloud, Yandex Disk, Google Drive, etc.; data of accounts synchronized via Microsoft or iCloud accounts (logins, passwords, etc.); applications of payment service providers and cryptocurrency exchanges installed on the device (active sessions, personal profile data, linked accounts, and transaction history); entries recorded in calendar and other planning applications; information on the presence of applications for remote device management; and the existence of external storage devices connected to computer ports[4].

4. The examined objects shall be packaged and sealed in compliance with security requirements, in the presence of a specialist and attesting witnesses. Where necessary, in order to block communications and restrict network connectivity, it is recommended to use a Faraday bag or, in the absence thereof, two layers of aluminum foil.

5. When items, documents, and electronic data are examined or seized, each such action shall be separately reflected in the official report, and the identifiers of electronic devices (IMEI and serial numbers) shall be recorded [5].

This issue becomes particularly relevant in the context of the high technical complexity of the digital environment. Electronic information is characterized by instability, the possibility of remote destruction or modification, and dependence on

software and hardware storage conditions. This requires law enforcement authorities not only to strictly comply with procedural norms, but also to take into account the technical characteristics of electronic data carriers, as well as to apply specialized knowledge and modern forensic methods.

In this regard, compliance with procedural requirements in the seizure of electronic information carriers serves as a fundamental guarantee for the protection of the rights and legitimate interests of citizens, as well as a condition for maintaining a balance between the objectives of criminal prosecution and the principles of fair trial. An analysis of certain aspects of the procedural seizure of electronic data carriers makes it possible to identify existing problems in law enforcement practice and to determine directions for its further improvement in light of the contemporary challenges of the digital era.

REFERENCES:

1. Article 205. Peculiarities of collection, verification and evaluation of electronic (digital) evidence Criminal Procedure Code of the Republic of Uzbekistan (Source: http://lex.uz).
2. The international standard ISO/IEC 27037:2012 (*Guidelines for identification, collection, acquisition and preservation of digital evidence*).
3. Article 95[1]. Peculiarities of collection, verification and evaluation of electronic (digital) evidence Criminal Procedure Code of the Republic of Uzbekistan (Source: http://lex.uz).
4. Ian Whiffin. 10 Best Practices for Digital Evidence Collection (Source: https://cellebrite.com/en/10-best-practices-for-digital-evidence-collection).
5. The Investigator's Desk Guide for Conducting Criminal Cases in the Field of Information Technologies. Methodological Manual. Law Enforcement Academy. Tashkent, 2025, pp. 36–40.