International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 5, Issue 4, April - 2026
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Procedural Forms of Collecting Digital Evidence: Inspection, Copying and Sampling for Expert Examination

Musurmonov Begzod Rakhimovich,
Researcher of the Law Enforcement
Academy of the Republic of Uzbekistan
E-mail: raximovichbekzod@gmail.com

Abstract

This article examines the core procedural forms of collecting digital (electronic) evidence in criminal proceedings: inspection of devices and electronic data, creation of a forensic bit-by-bit image-расм, and sampling/collection of parameters for expert examination (control samples, metadata and hash values). In Uzbekistan, the adoption of Law No. ЎРҚ-1003 and the Plenum of the Supreme Court Resolution of 23 June 2025 No. 14 have strengthened admissibility requirements for electronic data, including the need to document inspection, to issue a procedural decision on joining electronic materials to the case, and—where necessary—to appoint expert examination. The paper clarifies the meaning of integrity, authentication and chain of custody and shows how these criteria are operationalized through protocols, decisions and expert procedures. A comparative perspective draws on U.S. case law (Riley, Carpenter, Vayner, Griffin) and widely used digital-forensics models. Using examples from Supreme Court of Uzbekistan practice reviews, the article demonstrates that procedural defects in documenting and verifying evidence may lead to annulment of judicial decisions. The conclusion proposes de lege ferenda measures: investigator checklists, standardized chain-of-custody logs, and stronger participation of digital-forensics specialists.

Keywords: Digital evidence, electronic data, inspection, forensic copy, hash value, authentication, forensic examination.

Introduction

Digital technologies have radically changed the methods and traces of crime: through mobile devices, messengers, social networks, cloud services, geolocation and traffic data, a large amount of data on a person's movements and communications is being generated. In such conditions, electronic data in many cases becomes a decisive means of proof in investigative practice. However, the fact that digital evidence can be easily copied, edited, remotely controlled and reconstructed through metadata requires a high level of procedural discipline in their collection

and formalization [1, -B 118; 2, -B 123]. In order to legally strengthen this area in Uzbekistan, Law No. O‘RQ-1003-1 was adopted on November 21, 2024, and updates were made to the procedural rules aimed at determining the stages of working with digital evidence [4]. Also, by the Resolution of the Plenum of the Supreme Court No. 14 of June 23, 2025, the explanations on the admissibility of evidence were updated, and in order to use electronic data as admissible evidence: (a) it must be determined who, when, where and under what circumstances found/created them; (b) a report on the examination must be drawn up; (c) there must be a decision (ruling) on the inclusion of electronic data in the case; and, if necessary, an examination may be ordered [5, -B 3].

The purpose of the article is to scientifically and practically analyze the three main procedural forms of collecting digital evidence (examination, copying, sampling for examination), link them with assessment criteria (integrity, authentication, chain of custody), and develop proposals for improving national legislation and practice.

The study used formal-legal, systematic, comparative-legal, and doctrinal analysis methods. Using the formal-legal method, the provisions of the Code of Criminal Procedure, Law No. O‘RQ-1003 and Plenum resolutions on obtaining and ensuring the admissibility of digital evidence were analyzed [4; 5, -B 2–3; 6, 10]. The systematic analysis served to study other institutions in the system of proving digital evidence - investigative actions, examination, judicial control and the consequences of inadmissibility of evidence [1, -B 124–125]. Within the framework of the comparative-legal method, the authentication of electronic evidence and guarantees for access to digital information in US judicial practice (Riley; Carpenter; Griffin; Weiner) were analyzed, and conclusions were drawn for national development [12, -B 1–2; 13, -B 1–3; 14, -B 1–2; 15, -B 1–3]. Doctrinal analysis has focused on the scientific substantiation of the content of special criteria for evaluating digital evidence - integrity, authentication and chain of custody [1, -B 124–125; 3, -B 4–5; 8, -B 319].

In the scientific literature, two directions are visible in explaining digital evidence: the first approach considers digital evidence as an "electronic version" of traditional types of evidence; the second approach suggests that it should be regulated as an independent institution in a separate regime due to the characteristics of the digital environment. Voronin, recognizing that electronic evidence is assessed in practice according to general rules, emphasizes that courts often make errors in conclusions due to the fact that they do not take into account the risks inherent in the digital nature of evidence [1, -B 118]. Shushenachev points out that due to the inherent risks in the process of presenting digital information as evidence, the methods of its collection and recording (seizure, copying, osmosis) should be clearly regulated by law [2, -B 123–124]. Kolichenko notes that the problem of examining and evaluating electronic evidence lies in the insufficient standardization of procedural mechanisms [3, -B 4–5].

The procedural status of digital evidence in national legislation has been strengthened by recent reforms. The Plenum Resolution No. 14 of June 23, 2025 establishes the conditions for the use of electronic data, photo, audio, video recordings as admissible evidence, and clearly explains that a decision (ruling) should be made on their inclusion in the case as material/written/digital evidence after the report of their examination [5, -B 3]. This approach requires considering digital evidence not as a “file”, but as factual information that is introduced into the evidentiary system through a set of procedural actions.

Although the general criteria for digital evidence (relevance, admissibility, reliability, sufficiency) are maintained, three specific criteria are of decisive importance in practice due to the risks inherent in the digital environment: (1) integrity, (2) authentication, (3) chain of custody. According to Voronin, the reliability of electronic evidence can be correctly assessed only when the characteristics inherent in its digital nature are taken into account [1, -B 124–125]. Kolichenko also emphasizes that the reliability and admissibility of electronic evidence depend on the accuracy of the "verification-evaluation" procedures in practice [3, -B 5].

Kyei et al., by comparing digital forensic models, show that every action from the moment evidence is received to its presentation to the court must be documented and monitored; this is a substantive interpretation of chain of custody [8, -B 319]. From this point of view, it is not correct to limit integrity to the hash value alone: hashing is one of the means of proving integrity, but its procedural value is manifested in the documentation of who received the evidence, what equipment and in what order it was copied, and the packaging-storage-transfer documents [2, -B 124–125]. Inspection is the first stage of collecting digital evidence and in practice requires considering the "device" (physical carrier) and the "information" (digital content) as separate objects. According to the Plenum's explanations, in order to recognize electronic data as admissible evidence, it is necessary to determine who, when, where and under what circumstances found/created them, as well as draw up a report on the inspection [5, -B 3]. Thus, the investigator must at least reflect the following in the report: (a) device type and identifiers (IMEI/serial number, SIM/account information); (b) a list of files and data found/viewed; (c) software tools used; (d) photo and video recording devices; (e) measures to ensure that the data is not accidentally changed (airplane mode, disconnection from the network, blocking) [2, -B 124]. In judicial practice, shortcomings in procedural documentation can lead to the annulment of court decisions. For example, the Supreme Court case law reviews cite cases where the failure to sign the minutes of a court session was considered a serious violation of the norms of the Code of Criminal Procedure and resulted in the annulment of the verdict/ruling (case No. 1-1806-2101/11) [18, -B 7]. This example also illustrates a general rule for digital evidence: if the minutes and decisions are not fully and correctly executed, the risk of electronic data being excluded from the case or found inadmissible increases [1, -B 125]. The volatile nature of digital evidence makes it more preferable for the investigator to work with a "forensic copy" than "working with the original device". In forensic practice, by making a bit-by-bit image copy, all sectors of the data (including traces of deleted data) are preserved and an opportunity is created for subsequent verification [8, -B 319]. In this case, the hash value (for example, SHA-256) serves as a means of verifying the exact correspondence of the copy and the original [8, -B 320]. Shushenachev, emphasizing the requirement for procedurally correct formalization of the process of copying digital information, shows that the conditions under which the copying was carried out, by whom and with what means directly affect the admissibility of the evidence [2, -B 125].

Taking samples for examination (control sample, reference copy from an electronic carrier, metadata, used hash values) plays an important role in ensuring the authentication and integrity of digital evidence. According to the explanations of the plenum, in cases where necessary, an appropriate examination may be appointed to resolve the issue of including the submitted electronic data in the case [5, -B 3]. Kolichenko emphasizes the importance of expert examination in verifying the authenticity and integrity of electronic evidence, noting the need to clearly

formulate questions and correctly identify the objects of examination when assigning an examination [3, -B 14–15].

Comparative analysis allows for a better understanding of legal guarantees and authentication standards when working with digital evidence. In Riley v. California, the US Supreme Court stated that since digital data on a mobile phone poses a significant privacy risk, searches should generally not be permitted without a warrant [12, -B 1–2]. In Carpenter v. United States, the requirement of a court order for obtaining long-term geolocation (CSLI) data was also strengthened as a legal guarantee [13, -B 5–6]. These approaches link the criterion of "lawfulness" in the collection of digital evidence with procedural control.

In the authentication of materials obtained from social media/internet sources, Griffin v. State held that a screenshot alone is not sufficient and that additional corroborating evidence is required [14, -B 1–2]. United States v. Weiner also held that a web page must be accompanied by credible evidence linking it to the accused in order to be admissible as evidence [15, -B 2–3]. In national practice, this conclusion suggests the need to use metadata, logs, provider information, and expert opinion as practical foundations for authentication [1, -B 125; 5, -B 3].

The easy variability and multiplicity of digital evidence limit their mechanical assessment by traditional evidentiary logic; to ensure reliability, integrity, authentication and chain of custody criteria must be applied together [1, -B 124–125; 8, -B 319].

The fact that in the national legal order a report of inspection and a decision (decision) on the inclusion of electronic information in the case for the use of electronic information as admissible evidence strengthens the discipline of documentation in investigative practice [5, -B 3].

Real cases in the reviews of judicial practice (for example, case No. 1-1806-2101/11) show that shortcomings in procedural documentation lead to the annulment of court decisions; in the case of digital evidence as well, the report, decision and documents of acceptance and delivery are the "basic evidentiary infrastructure" [18, -B 7].

De lege ferenda suggestions (checklist for investigation):

a) When an electronic device is found: disconnect from the network/airplane mode, record the screen state in a photo-video format, enter IMEI/serial numbers in the report.

b) When copying information: take a forensic image, hash (SHA-256), display the copy and original hashes in the report, record the software used (with version).

c) Chain of custody journal: keep a uniform record of each receipt-delivery operation (from whom to whom, when, where, in what packaging).

g) When assigning an expert examination: clearly identify the object, clearly state the questions in technical and legal terms (metadata, signs of change, messenger/cloud logs), provide sufficient materials to draw a conclusion.

These proposals will ensure uniform practices in the collection and evaluation of digital evidence, reduce the risk of electronic data being deemed inadmissible, and strengthen safeguards in line with judicial review requirements.

REFERENCES

1. Voronin M. I. Osobennosti otsenki elektronnых (sifrovых) dokazatelstv // Aktualnые problemы rossiyskogo prava. 2021. T. 16. № 8 (129). S. 118–128. DOI: 10.17803/1994-1471.2021.129.8.118-128.

2. Shushenachev A. V. Pravovoye regulirovaniye sbora sifrovoy informatsii s selyu yee predstavleniya kak dokazatelstva v rassledovanii prestupleniy // Yuridicheskaya nauka. 2023. № 1. S. 122–126.
3. Kolichenko A. A. Problemы proverki i otsenki elektronnыx dokazatelstv v sovremennom ugolovnom protsesse: avtoref. dis. … kand. yurid. nauk (5.1.4). Nijniy Novgorod, 2024. 34 s.
4. O‘zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida: Qonun, 21.11.2024-y., O‘RQ-1003-son. URL: https://lex.uz/docs/7228758 (murojaat sanasi: 09.03.2026).
5. O‘zbekiston Respublikasi Oliy sudi Plenumining qarori: 2025-yil 23-iyun, № 14 (dalillar maqbulligiga oid jinoyat-protsessual qonuni normalarini qo‘llashga oid qarorga o‘zgartish). URL: https://sud.uz/wp-content/uploads/2025/07/plenum/14-son-Dalillar-ozgartirish-uz.pdf (murojaat sanasi: 09.03.2026).
6. O‘zbekiston Respublikasi Oliy sudi Plenumining qarori: 2018-yil 24-avgust, № 24 “Dalillar maqbulligiga oid jinoyat-protsessual qonuni normalarini qo‘llashning ayrim masalalari to‘g‘risida”. URL: https://lex.uz/ru/docs/3895986 (murojaat sanasi: 09.03.2026).
7. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi. URL: https://lex.uz/docs/111463 (murojaat sanasi: 09.03.2026).
8. Kyei K., Zavarsky P., Lindskog D., Ruhl R. A Review and Comparative Study of Digital Forensic Investigation Models // ICDF2C 2012. LNICST 114. 2013. P. 314–327.
9. Kalancha I., Bozhyk V., Muzychenko O., Vatsyk V. Digital Evidence in Comparative Criminal Procedure: International Experience and the Practice of Judicial Review // Transactions on Maritime Science (TPM). 2025. Vol. 32. No. S2. URL: https://www.tpmap.org/ (мурожаат санаси: 09.03.2026).
10. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007). URL: https://www.jenner.com/a/web/wwashvLFr57td3SAKeKQpH/4HRMZQ/Lorraine_v._Markel.pdf (accessed: 09.03.2026).
11. Riley v. California, 573 U.S. 373 (2014). URL: https://supreme.justia.com/cases/federal/us/573/13-132/case.pdf (accessed: 09.03.2026).
12. Carpenter v. United States, 585 U.S. ___ (2018). URL: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (accessed: 09.03.2026).
13. Griffin v. State, 19 A.3d 415 (Md. 2011). URL: https://www.courts.state.md.us/data/opinions/coa/2011/74a10.pdf (accessed: 09.03.2026).
14. United States v. Vayner, 769 F.3d 125 (2d Cir. 2014). URL: https://www.casemine.com/judgement/us/5914f5e2add7b0493498cb46 (accessed: 09.03.2026).
15. Federal Rules of Evidence, Rule 902 (Self-authentication). URL: https://www.law.cornell.edu/rules/fre/rule_902 (accessed: 09.03.2026).
16. Convention on Cybercrime (Budapest Convention), ETS No. 185 (23.XI.2001). URL: https://rm.coe.int/1680081561 (accessed: 09.03.2026).
17. Isakov A. A. TERGOVNI TO‘LA, HAR TOMONLAMA VA HOLISONA OLIB BORILISHINI TA’MINLASH // Development of Pedagogical Technologies in Modern Sciences (International scientific-online conference). 2024. DOI: 10.5281/zenodo.15966663.
18. O‘zbekiston Respublikasi Oliy sudi Rayosatining 2023-yil 27-oktyabrdagi RS-51-23-sonli qaroriga ilova: 2023-yil III chorak bo‘yicha sud amaliyoti obzori. URL: https://sud.uz/wp-content/uploads/2023/10/%D0%A0%D0%A1-51-23%20%D0%B8%D0%BB%D0%BE%D0%B2%D0%B0.pdf (murojaat sanasi: 09.03.2026).