

Date: 11th October-2026

DIGITAL EVIDENCE IN THE INVESTIGATION OF COMPUTER CRIMES: A FORMAL MODEL OF THE CHAIN OF CUSTODY AND A COMPARATIVE ANALYSIS OF ATTRIBUTION METHODS

Odilov O.F.^{1,a}, Bobonazarova M.Sh.^{1,b},
Nuraliyev Sh.Sh.^{1,c}, G'ulomov A.G'.^{1,d}

¹Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Abstract. This article examines the evidentiary stage of the response to computer crime, at which a technically established fact must be converted into a fact admissible in criminal proceedings. A five-stage model of the handling of digital evidence — identification, collection, preservation, analysis and presentation — is constructed, and the continuity of custody is formalised as a chain of cryptographic hash commitments in which every transfer between custodians is bound to a verified value. Admissibility is stated as a conjunction of four conditions covering the lawfulness of acquisition, the integrity of the object, the reproducibility of the method and the demonstrability of the inference, and it is shown that integrity alone, which receives the greatest technical attention, satisfies only one of them.

Keywords: digital evidence, computer forensics, chain of custody, admissibility of evidence, attribution, hash function, anti-forensics, electronic evidence, expedited preservation, mutual legal assistance.

Annotatsiya. Ushbu maqolada kompyuter jinoyatlariga qarshi kurashning isbot bosqichi — texnik jihatdan aniqlangan holatni jinoyat protsessida qabul qilinadigan dalilga aylantirish bosqichi tahlil qilinadi. Raqamli dalillar bilan ishlashning besh bosqichli modeli — aniqlash, yig'ish, saqlash, tahlil va taqdim etish — ishlab chiqiladi hamda dalillar saqlanish zanjirining uzluksizligi har bir topshirish tekshirilgan xesh qiymatiga bog'lanadigan kriptografik majburiyatlar zanjiri sifatida formallashtiriladi.

Kalit so'zlar: raqamli dalil, kompyuter kriminalistikasi, dalillar saqlanish zanjiri, dalilning yo'l qo'yilishi, atribusiya, xesh funksiya, antikriminalistika, elektron dalil, tezkor saqlash, o'zaro huquqiy yordam.

Introduction. The response of the state to a computer crime consists of two tasks that are frequently conflated. The first is technical: to establish what occurred, by what means and from which systems. The second is procedural: to convert that technical finding into evidence that a court will accept and upon which a conviction may lawfully rest. The two tasks obey different criteria. A technical reconstruction is satisfactory when it explains the observed artefacts; evidence is satisfactory when it has been obtained lawfully, when its integrity from the moment of seizure is demonstrable, when the method by which it was examined is reproducible by another expert and when the inference drawn from it excludes competing explanations. A technically impeccable investigation can fail entirely at the



Date: 11th October-2026

second stage, and investigations do fail in this way with a regularity that the technical literature rarely acknowledges.

The practical significance of this gap grows with the volume of offending. More than one million complaints were recorded by the Internet Crime Complaint Center in 2025 against losses of 20.9 billion United States dollars [1], and in the Republic of Uzbekistan the number of registered offences in the sphere of information technologies reached 58,800 in 2024 [2]. Each registered offence generates digital traces across several custodians — the victim's device, the operator's logs, a payment institution, a foreign hosting provider — and each of these traces is volatile, readily altered and, in many cases, held outside the jurisdiction conducting the investigation. The mean interval between the occurrence of an intrusion and its identification and containment is 247 days [3], by which time a substantial part of the trace material has been overwritten in the ordinary course of operation.

Two further circumstances aggravate the problem. The first is the deliberate destruction of traces by offenders, which in the phase model of a computer crime is not an incidental act but a constituent phase of the offence. The second is the growth of techniques that make the generation of persuasive but false material inexpensive: synthetic audio and video are now the most frequently encountered form of artificial-intelligence-assisted attack [3], and material produced in this way may enter the evidentiary record as readily as it enters a fraudulent transaction. The evidentiary question is thus no longer only whether a given artefact has been altered since seizure but whether it was authentic when created.

The contribution of this article is fourfold. First, a five-stage model of the handling of digital evidence is constructed and the continuity of custody is formalised as a chain of cryptographic commitments. Second, admissibility is stated as a conjunction of four conditions, and it is shown which of them the usual technical practice does and does not satisfy. Third, a four-level scale of attribution is proposed and the limits of technical attribution are established. Fourth, the methods of attribution are compared with respect to the level they support and to their resistance to falsification, and the cross-border problem is assessed against the available instruments of international cooperation.

Literature review and methodology. The discipline acquired its structure at the first Digital Forensic Research Workshop, whose report defined the process as a sequence of identification, preservation, collection, examination, analysis and presentation, and established the principle that each stage must be documented to a standard permitting independent repetition [4]. Casey subsequently provided the systematic treatment of the relation between technical findings and legal proof, and introduced a scale for expressing the certainty of a digital finding that remains the reference for the expression of conclusions in expert reports [5].

The standardisation of practice followed. The National Institute of Standards and Technology published guidance integrating forensic techniques into incident response [6]; the International Organization for Standardization issued a family of standards covering the identification, collection, acquisition and preservation of digital evidence and the



Date: 11th October-2026

subsequent investigation process [7, 8]. Garfinkel, reviewing the first decade of the field, identified the approaching crisis of scale: the growth in the volume of storage, the diversity of devices and the spread of encryption were, he argued, outpacing the development of methods, so that the examination of a single case would become infeasible within the time available to an investigation [9]. That prediction has been borne out, and it supplies part of the motivation for the present analysis, since a model of the evidentiary process is of practical value only if it indicates where effort must be concentrated when complete examination is impossible.

On attribution, the authoritative treatment is that of Rid and Buchanan, who argued that attribution is not a technical problem admitting a binary answer but a multi-layered process combining technical, operational and strategic evidence, in which the degree of confidence must be stated explicitly and is never absolute [10]. This position underlies the scale proposed below. The counterpart literature on anti-forensics, systematised by Harris, classifies the techniques by which an offender destroys, conceals, falsifies or renders unusable the traces of conduct [11], and it is used here to assess the resistance of each attribution method to deliberate manipulation.

Two gaps are apparent. The technical standards specify what must be done at each stage but do not state the conditions under which the resulting material is admissible, which are determined by procedural law and differ by jurisdiction; conversely, the procedural literature states the conditions but does not connect them to the technical operations that satisfy them. And attribution is commonly discussed as though it were a single question, whereas the evidentiary requirements for identifying a device, an account, a person and a responsible actor differ fundamentally. The analysis that follows addresses both gaps.

The methodology is analytical and comparative. A reference model of the evidentiary process is constructed and its integrity requirement is formalised. The conditions of admissibility are then stated as a predicate and each condition is mapped to the operations that satisfy it. A scale of attribution is constructed and the available methods are evaluated against it with respect to the level supported and to resistance against anti-forensic manipulation. Finally the model is applied to the cross-border case, which is the normal rather than the exceptional configuration in this category of offence. The material consists of published standards, procedural legislation and the scientific literature; no primary data were collected by the authors.

Reference model of the handling of digital evidence. The process is modelled as a sequence of five stages, shown in Figure 1. The model differs from the classical formulations in one respect: the integrity checkpoints are represented explicitly as a layer above the stages, because it is the continuity of that layer, and not the correctness of any individual stage, that determines whether the material survives challenge.



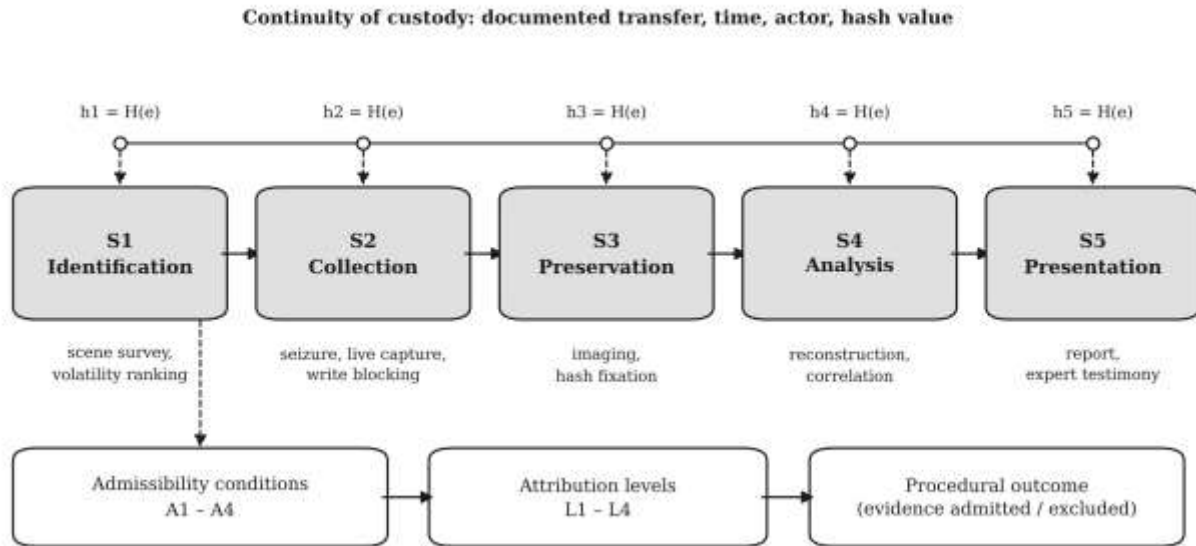


Figure 1. Reference model of the handling of digital evidence with integrity checkpoints and continuity of custody

At the identification stage (S1) the objects carrying relevant traces are located and ranked by volatility, since the order of collection determines what survives: the contents of memory, network connections and running processes are lost on power interruption, whereas data on non-volatile storage persist. The ranking is not a technicality but a decision with evidentiary consequences, because evidence of the execution of malicious code frequently exists only in memory. At the collection stage (S2) the objects are seized or captured, with write protection applied to storage media and live acquisition performed where the system cannot be interrupted. At the preservation stage (S3) a forensic image is produced and its hash value fixed in the record of proceedings. All subsequent examination is performed on copies of the image, never on the original. At the analysis stage (S4) the events are reconstructed from the artefacts and correlated across sources. At the presentation stage (S5) the findings are expressed in a report and, where necessary, in expert testimony, in a form intelligible to a reader without technical training.

The continuity of custody is formalised as follows. Let e denote the object of evidence and H a collision-resistant hash function. At the moment of fixation a value

$$h_0 = H(e)$$

is computed and entered in the record of seizure together with the time, the identity of the person performing the operation and the technical means employed. Each subsequent transfer of the object from custodian k to custodian $k+1$ produces a further entry

$$T_k = (h_k, \tau_k, id_k, id_{k+1}, m_k), \text{ with } h_k = H(e_k),$$

where τ_k is the time of transfer, id_k and id_{k+1} the transferring and receiving custodians and m_k the method of verification. The chain is intact when

$$h_0 = h_1 = \dots = h_n \text{ and the sequence } \tau_0 \leq \tau_1 \leq \dots \leq \tau_n \text{ is continuous without gaps.}$$

Two properties of this construction deserve emphasis. The first is that the equality of hash values establishes that the object has not changed since h_0 was computed; it

Date: 11th October-2026

establishes nothing whatever about the period before that moment. If the object was altered prior to fixation — by the offender, by an incautious system administrator attempting to restore service, or by the ordinary operation of the system — the chain will be perfectly intact and will attest to the integrity of material that is already corrupted. The second is that the continuity of the time sequence carries independent evidentiary weight: an unexplained interval during which the object was not in documented custody is sufficient to found a challenge even where the hash values match, because the hash demonstrates identity of content and not the impossibility of substitution at an earlier stage. These two observations explain why the practical centre of gravity of evidentiary work lies at the first minutes after discovery, and not in the laboratory.

Conditions of admissibility. The acceptance of digital material as evidence is modelled as a conjunction of four conditions. Let e be the object and R the record of proceedings concerning it. The material is admissible when:

- A1 (lawfulness of acquisition): the object was obtained by a procedural action provided for by law, carried out by an authorised official within the limits of an authorisation and documented in the prescribed form;
- A2 (integrity of the object): the chain of custody is intact in the sense defined above, that is, the hash values coincide and the time sequence contains no undocumented gaps;
- A3 (reproducibility of the method): the technique of examination is documented in sufficient detail, and the instruments employed are sufficiently validated, that an independent expert applying the same technique to the same object would obtain the same result;
- A4 (demonstrability of the inference): the conclusion drawn from the artefacts is stated with an explicit degree of certainty, and the competing explanations consistent with the same artefacts are identified and addressed.

The admissibility predicate is therefore

$$\text{Admissible}(e) = A1 \wedge A2 \wedge A3 \wedge A4.$$

The conjunctive form is the substance of the matter. Technical practice, and the commercial instruments that serve it, address A2 almost exclusively: hash computation, write blocking and verified imaging are mature, automated and inexpensive. Condition A1 is a matter of procedural discipline and is the most frequent cause of exclusion in practice, since the seizure of a device ordinarily requires a lawful basis and the collection of traffic or content data from an operator requires a separate one. Condition A3 is systematically underserved: the use of an instrument whose behaviour is not documented, or the performance of an examination whose steps are not recorded, produces a finding that cannot be independently repeated and that a competent defence will therefore contest successfully. Condition A4 is the one most often violated in expert reports, which habitually state conclusions categorically where the artefacts support only a probabilistic inference. A report asserting that a given person committed an act, where the artefacts establish only that a given account was used from a given device, misstates the strength of the evidence and exposes the entire finding to rejection.



Date: 11thOctober-2026

Levels of attribution. Attribution is not a single question. Four distinct assertions are commonly conflated under that name, and they differ both in the evidence required and in the procedural consequence. They are set out as a graduated scale in Table 1.

Table 1. Levels of attribution and the evidence required at each level

Level	Assertion established	Typical evidentiary basis	Resistance to falsification	Procedural significance
L1	A specific device or network node participated in the event	Network logs, addresses, device identifiers, artefacts of the file system	Low: addresses are readily substituted, proxies and botnets interpose third parties	Insufficient on its own; establishes a line of inquiry
L2	A specific account or set of credentials was used	Authentication logs, session records, operator data	Moderate: credentials are stolen and traded, so use does not imply ownership	Insufficient; requires evidence connecting the account to a person
L3	A specific natural person was in control of the account or device at the material time	Physical evidence of location, biometric and access records, correspondence, concurrent activity on other systems	Moderate to high where sources are independent	Necessary condition for charging a person
L4	That person committed the act with the requisite mental element	The whole body of evidence, including evidence outside the digital domain: preparatory acts, motive, disposal of proceeds, statements	High, since the sources are heterogeneous and difficult to falsify jointly	Sufficient basis for conviction

Note. The transition from L3 to L4 cannot be effected by technical means. No artefact establishes intention; the digital evidence establishes conduct, and the mental element is inferred from the totality of the circumstances in accordance with the general rules of proof.

The scale makes explicit a confusion that is the source of much unsound expert evidence. A finding at L1 is frequently reported as though it were a finding at L3. The intervening steps are non-trivial: an address identifies a point of connection and not a person, and in the ordinary architecture of this offending the point of connection belongs to an uninvolved third party whose device has been compromised precisely so that it should appear in the logs. The transition from L2 to L3 is the point at which the investigation must leave the digital domain, since the proposition that a particular person used a particular account is established by evidence of presence, of concurrent activity and of circumstance, and not by any property of the artefacts themselves.

The corollary for the construction of a case is that attribution is cumulative and must be built from independent sources. A single source at any level, however technically

Date: 11thOctober-2026

sound, supports a weaker inference than two mutually independent sources at a lower level, because independence is what defeats falsification: an offender who can manipulate one category of trace can rarely manipulate several categories consistently, and the detection of an inconsistency between sources is itself evidence of manipulation.

Anti-forensic conduct and its detection. Deliberate interference with traces is a constituent phase of the offence rather than an incidental consequence of it, and the methods employed fall into four classes which differ in the countermeasure they require.

Table 2. Classes of anti-forensic conduct and the corresponding countermeasures

Class	Method	Effect on the evidentiary process	Countermeasure
F1 Destruction	deletion of logs and files, secure erasure, clearing of journals	The object of evidence ceases to exist; condition A2 cannot be satisfied for it	Transfer of logs in real time to an append-only store outside the control of the compromised system
F2 Concealment	encryption, steganography, storage in unallocated areas, use of volatile memory only	The object exists but is inaccessible; the examination may exceed the time available	Live acquisition before shutdown; lawful means of obtaining keys; memory capture as a standard first step
F3 Falsification	alteration of file timestamps, fabrication of log entries, planting of artefacts pointing to a third party	The object exists and is intact since seizure but is untrue; conditions A2 and A4 diverge	Correlation of independent sources; comparison of internal timestamps with operator-side records
F4 Obstruction	exploitation of defects in forensic tools, generation of large volumes of spurious data, use of anonymising infrastructure	The examination becomes unreliable or infeasible within the available time; condition A3 is threatened	Validated instruments, examination by two independent tools, documented limitation of the scope of examination

Class F3 is the most consequential for the model developed above and the least addressed by existing practice. Falsified material passes every integrity check, because the chain of custody attests only to the absence of change after fixation. The only effective response is correlation across sources that are not under the offender's joint control: a timestamp within a file system may be set to any value, but it cannot be reconciled with the records of an operator or a payment institution unless those too have been altered. This is a

Date: 11th October-2026

further reason why the evidentiary weight of a finding rests on the independence of its sources rather than on the technical quality of any one of them.

The same consideration applies with new force to synthetic material. Where audio, video or documentary material may have been generated rather than recorded, the question posed to the expert changes from the integrity of the object to the authenticity of its origin, which is a different and harder question. In the terms of the model this is a failure of A4 rather than of A2: the artefact is intact and the inference drawn from it is unsound. The practical response is the systematic corroboration of such material by metadata from the capturing device, by records of its transmission and by the circumstances of its creation — that is, by the same principle of independent sources.

Evidence located in another jurisdiction. In this category of offence the evidence required is routinely held abroad: the victim is in one state, the server in a second, the account with the service provider in a third and the proceeds in a fourth. Two properties of digital evidence make this configuration more difficult than its analogue in traditional crime. The evidence is volatile, so that the interval between the request and its execution may exceed the retention period of the data sought; and it is not susceptible to unilateral acquisition, since an investigator who obtains data from a foreign system without the consent of that state acts outside the authorisation of the law and produces material inadmissible under condition A1.

The instruments available are of three kinds and differ in speed by orders of magnitude. The first is expedited preservation: a request that the holder of the data retain them pending a formal request for production. This is the decisive instrument in practice, because it is fast and because it converts a volatile object into a stable one; the Council of Europe Convention on Cybercrime establishes it in Articles 16, 17 and 29 together with a network of contact points available at all hours [12]. The second is mutual legal assistance proper, by which the data are produced for use in proceedings; it is reliable but slow, and the interval commonly exceeds the retention periods of the holders. The third is direct cooperation with service providers, which is rapid but limited in the categories of data that may be obtained voluntarily, and which does not extend to content.

The United Nations Convention against Cybercrime, adopted by the General Assembly in December 2024 and opened for signature at Hanoi on 25 October 2025, extends an equivalent framework to a global membership, with provisions on expedited preservation, production orders, search and seizure, real-time collection of traffic data, extradition and twenty-four-hour contact points [13]. Its significance for states that are not parties to the earlier instrument is practical rather than declaratory: it creates a channel where none existed, and the absence of such a channel has been the ordinary reason for the discontinuance of cross-border investigations. The criticisms directed at the convention — that the range of conduct covered is defined broadly and that the human-rights safeguards are remitted to national law — are directed at precisely the questions that national implementing legislation must settle, and they are therefore an argument for careful implementation, including judicial authorisation for intrusive measures and a defined regime for the refusal of requests.

Date: 11th October-2026



Procedural requirements under the law of the Republic of Uzbekistan. Digital material enters criminal proceedings in the Republic of Uzbekistan through the general provisions of the Code of Criminal Procedure governing evidence, its sources and the procedural actions by which it is obtained [14]. Material objects carrying traces of an offence are examined and attached to the case as physical evidence, and the seizure of devices, the examination of premises and the obtaining of information from operators are carried out by the corresponding procedural actions, with judicial authorisation where the action restricts a constitutional right. In the terms of the model, these requirements constitute condition A1, and the procedural form of the record of seizure is also the instrument that establishes the first link of the chain of custody: the hash value and the time of fixation are entered in it, and the evidentiary value of the whole subsequent chain depends on that entry being made correctly at the outset.

The substantive qualification of the conduct under investigation is governed by Chapter XX¹ of the Criminal Code, which establishes liability for offences in the sphere of information technologies in Articles 278¹–278⁶ [15], and by the general provisions on offences against property where the object of the encroachment is property. Conduct falling within class F1 of Table 2 — the destruction of traces — is itself capable of constituting a separate offence, both as the modification or destruction of computer information and as the concealment of a crime, a circumstance of practical importance because it permits the investigation to be directed at the concealment phase where the principal offence is difficult to prove.

The obligations of operators are of direct evidentiary consequence. The Law 'On Cybersecurity' establishes the system of cybersecurity subjects and the requirements applicable to critical information infrastructure [16]; the Law 'On Informatisation' governs the activity of information system operators [17]; and the Law 'On Personal Data' governs the processing of personal data and the conditions of their transfer [18]. From the standpoint of the present model these instruments determine the availability of evidence: what is logged, for how long it is retained and under what conditions it may lawfully be handed over. An investigation cannot obtain what was never recorded, and the retention period of operator records is therefore a binding constraint on the investigative capability of the state. The task of creating a system for countering cybercrime set by the Strategy of Development of New Uzbekistan for 2022–2026 [19] accordingly implies, on the evidentiary side, a defined minimum of logging for operators of essential services, protection of the integrity of those logs against the conduct of class F1, and an institutional capability to transmit and to execute requests for expedited preservation within hours rather than weeks.

Discussion. Three conclusions of practical consequence follow from the analysis.

The first is that the evidentiary strength of a digital finding is determined by the weakest of the four admissibility conditions and not by the strength of the technical work. Because the conditions are conjunctive, effort devoted to the condition already satisfied yields nothing. The present distribution of effort is the inverse of the rational one: integrity, which is automated and inexpensive, receives the greatest attention, while reproducibility

Date: 11th October-2026

of method and the demonstrability of the inference, which depend on documentation and on the discipline of expression, receive the least and are the conditions upon which cases are in practice lost.

The second is that the limit of technical attribution lies at the third level of the proposed scale. Digital artefacts can establish that a device participated, that an account was used and, in combination with evidence of circumstance, that a particular person was in control of that account; they cannot establish the mental element of the offence. An expert report that states a conclusion at the fourth level exceeds the competence of the expert and, by misstating the strength of the evidence, imperils the finding at the levels that were in fact established. The correct discipline is to state the level reached and the degree of certainty attaching to it, leaving to the investigator and the court the inference that the scale does not support.

The third is that the decisive variable in cross-border cases is institutional latency rather than legal competence. The instruments of preservation and assistance exist; what determines whether evidence survives is whether a request for preservation can be issued and executed within the retention period of the holder, which is measured in days or weeks. Investment in the capacity to act quickly — a contact point available at all hours, standard forms, officers trained to issue preservation requests without awaiting the completion of formal procedures — therefore dominates investment in any technical capability, because no analytical capacity can examine material that has already been overwritten.

Several limitations of this study should be stated. The admissibility conditions are formulated at a level of generality intended to apply across procedural systems, and their precise content in a given jurisdiction is determined by that jurisdiction's law and judicial practice; the article does not analyse judicial decisions, and an empirical study of the grounds on which digital evidence is in fact excluded would be required to establish the relative frequency of failure of each condition. The scale of attribution is qualitative and does not assign numerical confidence to its levels. The treatment of synthetic material is preliminary, since methods for establishing the authenticity of origin are developing rapidly and no standard practice has yet emerged. Finally, the analysis assumes that the holder of the evidence is identifiable, which is not the case where infrastructure is distributed across anonymising networks.

These limitations indicate the direction of further work. The authors intend to analyse the grounds of exclusion of digital evidence in published judicial practice, to develop a template for expert reports that requires the explicit statement of the attribution level and of the degree of certainty, and to assess the retention periods applied by operators in the national segment against the intervals actually required to issue and execute a request for preservation.

Conclusion. This article has examined the evidentiary stage of the response to computer crime and has formalised the handling of digital evidence as a five-stage process whose continuity of custody is expressed as a chain of cryptographic commitments. It was shown that the equality of hash values establishes integrity only from the moment of



Date: 11th October-2026

fixation and says nothing about the preceding period, from which it follows that the evidentiary centre of gravity lies in the first minutes after discovery rather than in the laboratory.

Admissibility was stated as a conjunction of four conditions — lawfulness of acquisition, integrity of the object, reproducibility of the method and demonstrability of the inference — and it was established that technical practice addresses principally the second, while cases are in practice lost on the first, third and fourth. A four-level scale of attribution was proposed, and it was demonstrated that the transition from the identification of a person in control of an account to the establishment of responsibility for the act cannot be accomplished by technical means and requires evidence outside the digital domain.

The classes of anti-forensic conduct were compared, and it was shown that falsification defeats integrity verification entirely, so that the weight of a finding rests on the independence of its sources rather than on the technical quality of any one of them — a conclusion that extends directly to synthetic material, where the question at issue is the authenticity of origin rather than the absence of subsequent change. For evidence located abroad, expedited preservation was identified as the decisive instrument and institutional latency as the binding constraint. The requirements of the criminal procedure legislation of the Republic of Uzbekistan and of the relevant international standards were substantiated, and the significance of the United Nations Convention against Cybercrime for the obtaining of cross-border evidence was indicated.

REFERENCES:

1. Internet Crime Report 2025. – Washington: Internet Crime Complaint Center, Federal Bureau of Investigation, 2026.
2. On the state of crime in the sphere of information technologies: data of the Ministry of Internal Affairs of the Republic of Uzbekistan for 2019–2024. – Tashkent, 2025.
3. Cost of a Data Breach Report 2026. – Armonk: IBM Security, 2026.
4. Palmer G. A Road Map for Digital Forensic Research: Report from the First Digital Forensic Research Workshop (DFRWS). – Utica, New York, 2001. – 48 p.
5. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. – Waltham: Academic Press, 2011. – 840 p.
6. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response: NIST Special Publication 800-86. – Gaithersburg: National Institute of Standards and Technology, 2006. – 121 p.
7. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. – Geneva: ISO, 2012. – 46 p.
8. ISO/IEC 27043:2015. Information technology — Security techniques — Incident investigation principles and processes. – Geneva: ISO, 2015. – 30 p.
9. Garfinkel S.L. Digital forensics research: The next 10 years // Digital Investigation. – 2010. – Vol. 7, Supplement. – P. S64–S73.



Date: 11th October-2026

10. Rid T., Buchanan B. Attributing Cyber Attacks // Journal of Strategic Studies. – 2015. – Vol. 38, No. 1–2. – P. 4–37.
11. Harris R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem // Digital Investigation. – 2006. – Vol. 3, Supplement. – P. 44–49.
12. Convention on Cybercrime, ETS No. 185. – Budapest: Council of Europe, 23 November 2001.
13. United Nations Convention against Cybercrime: adopted by General Assembly resolution 79/243 of 24 December 2024, opened for signature at Hanoi on 25 October 2025. – New York: United Nations, 2025.
14. Code of Criminal Procedure of the Republic of Uzbekistan of 22 September 1994, No. 2013-XII (as amended). – URL: <https://lex.uz/docs/111463>
15. Criminal Code of the Republic of Uzbekistan of 22 September 1994, No. 2012-XII (as amended), Chapter XX¹, Articles 278¹–278⁶. – URL: <https://lex.uz/docs/111457>
16. On Cybersecurity: Law of the Republic of Uzbekistan of 15 April 2022, No. ZRU-764. – National Database of Legislation of the Republic of Uzbekistan, No. 03/22/764/0330.
17. On Informatisation: Law of the Republic of Uzbekistan of 11 December 2003, No. 560-II (as amended). – URL: <https://lex.uz/ru/docs/82956>
18. On Personal Data: Law of the Republic of Uzbekistan of 2 July 2019, No. ZRU-547 (as amended). – URL: <https://lex.uz/ru/docs/4396428>
19. On the Strategy of Development of New Uzbekistan for 2022–2026: Decree of the President of the Republic of Uzbekistan of 28 January 2022, No. UP-60. – URL: <https://lex.uz/docs/5841063>
20. Carrier B. File System Forensic Analysis. – Upper Saddle River: Addison-Wesley, 2005. – 600 p.
21. Ayers R., Brothers S., Jansen W. Guidelines on Mobile Device Forensics: NIST Special Publication 800-101, Rev. 1. – Gaithersburg: National Institute of Standards and Technology, 2014. – 85 p.
22. Comprehensive Study on Cybercrime. – Vienna: United Nations Office on Drugs and Crime, 2013. – 320 p.
23. Quick D., Choo K.-K.R. Big forensic data reduction: digital forensic images and electronic evidence // Cluster Computing. – 2016. – Vol. 19, No. 2. – P. 723–740.
24. ENISA Threat Landscape 2025. – Athens: European Union Agency for Cybersecurity, 2025.

