Electronic Evidence in Criminal Procedure: Methods for Its Detection, Investigation and Legal Consolidation

Valeriia Shulha * [a], Lina Kaliuzhna ** [b]

* National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine, ORCID: https://orcid.org/0009-0000-7239-2494, e-mail: feup.Shulha@nupp.edu.ua

** National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine, e-mail: kalyuzhna1892@gmail.com

[a] Writing – original draft, project administration, supervision.
[b] Writing – original draft.

DOI: 10.32353/khrife.3.2025.?? UDC 343.9:004.056.5
Received: 23.07.2025 / Reviewed: 04.08.2025 / Accepted for print: 24.09.2025 / Available online: 30.09.2025

The paper presents a comprehensive analysis of electronic evidence in the context of criminal procedure. Its place and significance within the evidence system were determined. The authors explore the essence of electronic evidence, its nature and peculiarities of storage, recording and further investigation. Emphasis is placed on the fact that development of digital technologies opens up new possibilities for collecting evidence. Conversely, it also leads to problems related to the admissibility and authenticity of such data. The article outlines the main sources of electronic evidence, including computer systems, mobile devices, servers, cloud services, video surveillance cameras, e-correspondence and other objects that contain digital information. Current forensic methods of collecting electronic evidence, including methods of identification, recording and extraction of information from physical media, were studied. Stages and procedures that must be followed to ensure information remains unaltered—crucial for its admissibility in a trial—were outlined. The authors stress the need to conform to the principles of integrity, confidentiality and credibility when working with digital evidence. The procedural aspect was

This article is translation of the original Ukrainian content, which source is available at the link: *https://khrife-journal.org/index.php/journal* (translated by Daryna Dukhnenko). The author acknowledges translation as corresponding to the original.

given particular attention: the procedure for formalizing electronic evidence in compliance with the requirements of Ukraine's criminal procedural legislation. Current rules governing the procedures for collection, storage and provision of such evidence in court were analysed. The main issues in law application practice include insufficient regulation of issues regarding the preservation of electronic evidence, the difficulty of establishing its authenticity, and the risk of falsification. The study underscores the importance of improving legislative framework and introducing uniform standards for working with electronic evidence. The paper outlines proposals to optimize the collection and processing of electronic evidence, and to introduce modern technical means and software that comply with international standards.

Keywords: *electronic evidence; criminal procedure; criminalistics; digital technologies; evidence collection; procedural formalization; information security; authenticity; forensic digital examination.*

Research Problem Formulation

In light of society's digitalization and the increasing introduction of electronic technologies into everyday life, electronic evidence is becoming an essential component of criminal proceedings. Its features—specifically its intangible form, reliance on storage media and instability—necessitate the introduction of new methods for detecting, documenting and analysing such information.

The above features both increase the complexity of the procedure for the procedural formalization of electronic evidence and cast doubt on the authenticity and admissibility of corresponding materials in court. This is particularly the case if the rules for recording digital data are violated. A large share of evidence obtained from electronic sources demands specialized technical support during its collection. For this purpose, it is important to involve specialists in information technology (IT) and digital forensics.

Currently, Ukraine lacks systematic regulatory oversight in the criminal field. This oversight would cover all stages of working with electronic evidence: from initial extraction to procedural formalization. The Criminal Procedure Code of Ukraine [1] (CPC of Ukraine) contains neither any mention of digital objects nor an interpretation of the *electronic evidence* concept. Although, in Ukraine's national legal framework, the *electronic evidence* category was first legally enshrined in 2017 when the relevant provisions were incorporated into three main procedural codes: the Civil Procedure Code of Ukraine, the Economic Procedure Code of Ukraine and the Code of Administrative Proceedings of Ukraine (CAP of Ukraine). This has emerged as a pivotal point in the development of procedural law amid the digitalization of society and legal practice. All previously stated considerably complicates the work

1 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 25.06.2025).

of forensic experts, specialists, investigators and prosecutors, as well as raises questions about the admissibility of evidence obtained during a trial.

Article Purpose

Comprehensively analyse theoretical and practical aspects of applying electronic evidence in criminal procedure (within the scope of this objective, the following is planned: define the essence of electronic evidence; reveal the specifics of its identification, collection, recording, storage and analysis for criminalistics-related purposes; examine the procedural order for formalizing and using electronic evidence in court proceedings, taking into account the requirements of national legislation and international standards), identify challenging issues associated with the legal regulation, technical support and admissibility of electronic evidence in criminal proceedings, as well as put forward scientifically sound recommendations for improving the theory and practice of working with electronic evidence in the context of information technology development.

Research Methods

General scientific (analysis, synthesis, comparison and modelling) and special methods (formal-logical, comparative-legal, structural-functional and forensic) were utilized.

Analysis of Essential Researches and Publications

Electronic evidence as a subject of research has been extensively studied by M. Hutsaliuk et al. [2], O. Metelev [3], V. Muradov [4], M. Pashkovskyi [5], V. Romaniuk and T. Fomina [6], A. Skrypnyk [7], A. Stolitnii and I. Kalancha [8], and others. Researchers

2 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Вид. 2-ге, допов. Київ, 2020. 104 с. URL: https://surli.cc/klrpaf (date accessed: 25.06.2025).

3 Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства.* 2023. № 1—2. С. 42—53. DOI: 10.17721/2413-5372.2023.1-2/42-53 (date accessed: 25.06.2025).

4 Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. № 3-2. С. 316—318. URL: https://pap-journal.in.ua/wp-content/uploads/2020/09/3-2_2013.pdf (date accessed: 25.06.2025).

5 Пашковський М. І. Використання електронних (цифрових) доказів у кримінальних провадженнях про колаборaційну діяльність: практика судів Одеської області. *Протидія проявам тероризму та колаборaціонізму в умовах війни: стан та перспективи :* мат-ли Всеукр. кругл. столу (Кропивницький, 24.11.2023). Кропивницький, 2023. С. 42—48. URL: https://surl.lt/wpqxyo (date accessed: 25.06.2025).

6 Романюк В. В., Фоміна Т. Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колаборaційну діяльність. *Вісник Кримінологічної асоціації України*. 2024. Т. 32. № 2. С. 344—353. DOI: 10.32631/vca.2024.2.25 (date accessed: 25.06.2025).

7 Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Харків, 2022. 408 с.

8 Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2019. Вип. 146. С. 179—191. DOI: 10.21564/2414-990x.146.171218 (date accessed: 25.06.2025).

stress that there is no unified approach to the nature of electronic evidence. Most interpret it as a separate category, while others interpret it as a form of recording data that are to be classified in conformity with widely recognized sources (documents, physical evidence, testimony, expert opinions). They also note the lack of regulatory clarity regarding procedures for the extraction and recording of digital data. Analysis of judicial practice reveals an inconsistent approach to admitting electronic evidence. This is often due to errors during extraction, non-compliance with recording requirements, ambiguity of the source, etc.

Particularly challenging in this context is determining who had access to information, in which digital environment this information was created or modified, and how exactly it reached investigating authorities. Identifying the subject of access to digital data and its source remains one of the most complex tasks in working with electronic evidence. Electronic evidence should be considered in aggregate with technical conditions for its creation, authenticity, and procedural support: primarily through investigative actions (search, inspection and temporary access). It cannot be viewed as an abstract legal category.

Main Content Presentation

In modern criminal procedure, electronic evidence is becoming crucial as a tool for recording and supporting circumstances of an offense. Its specific nature requires the use of technical means to collect and analyse information. Furthermore, its procedural status should be legally consolidated as an independent type of evidence within the framework of criminal procedural legislation. From the perspective of criminal proceedings, evidence is recognised as factual data obtained in a well-defined procedural manner. Such data can be used by the authorised subjects in criminal proceedings—investigators, prosecutors, investigating judges or courts—to establish the presence or absence of facts and circumstances relevant to criminal proceedings and crucial for ascertaining truth in a case. Art. 84 of the CPC of Ukraine sets out this definition. It further enshrines an exhaustive list of sources of procedural evidence [9]. According to the law, sources shall be testimonies, physical evidence, documents and expert findings [10].

As set forth in Art. 98 of the CPC of Ukraine, physical evidence shall mean tangible objects that have been used as a tool for committing criminal offence, retain traces of such or contain other information, which may be used as evidence of the fact or circumstance to be established during criminal proceedings, including the items that were an object of criminally unlawful actions, money, valuables or other articles obtained in a criminally unlawful manner. In this sense, physical evidence plays a pivotal role as a material foundation for verifying and evaluating other sources of evidentiary information [11].

Documents occupy a special place in the evidentiary information structure, which, according to Art. 99 of the Criminal Procedure Code of Ukraine, may be recog-

9 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 16.07.2025).

10 Там само.

11 Там само.

nized as physical evidence provided that they contain information pertaining to identifying legally relevant facts. This rule emphasises that the legislator recognises both traditional physical media and modern electronic recording devices as documents, including photographs, video and audio recordings, as well as other media created and/or stored using computer technology. Furthermore, individual documents characterised by the immutability of their form and content may have a dual status: they can be considered both documentary and physical evidence [12].

Pursuant to the foregoing, electronic evidence in criminal proceedings should be viewed as a specific form of evidentiary information that is available in digital (intangible) format and is subject to recording, storage, processing and evaluation, taking into account both technical and legal aspects [13].

With this in mind, such evidence can be obtained using computer devices, servers, digital media or network sources, specifically the Internet. However, for further use in proving, such information requires special software or technical processing in order to convert it into a perceivable format.

In the context of current law application practice, the *digital evidence* term is often used alongside the *electronic evidence* term. Due to the lack of regulatory consolidation and clear distinction between these concepts, they are often used interchangeably, although some researchers suggest differentiating them as appropriate to the context: e.g., *electronic evidence* should be considered a formal procedural category, whereas *digital evidence* is a technical characteristic of a medium [14].

As set forth in the Law of Ukraine: *On Electronic Documents and Electronic Documents Circulation*, any information provided in a form suitable for its processing by electronic means is considered data. Such data may be of legal value and, provided the proper record, authentication and integrity, they serve as evidence in criminal proceedings [15].

From a technical perspective, such evidence can be stored on various digital media, such as external devices (specifically, memory cards, hard drives, mobile phones), internal or external servers, cloud storage, or backup systems, and in the virtual environment of the Internet. All this forms a new evidentiary reality in which a large portion of legally relevant information exists solely in digital format [16].

As we have previously mentioned (despite the lack of a clear definition in the CPC of Ukraine), digital evidence has grown to be an inherent part of trials. Its application expands the potential to prove a case; however, digital evidence requires special attention to issues of authenticity and admissibility. To ensure a balance between the interests of justice and the protection of human rights, detailed rules for proving

12 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 16.07.2025).

13 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Зазнач. твір. URL: https://surli.cc/klrpaf (date accessed: 25.06.2025).

14 Там само.

15 Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (date accessed: 22.07.2025).

16 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Зазнач. твір. URL: https://surli.cc/klrpaf (date accessed: 25.06.2025).

cases based on digital data are to be developed [17].

In addition, A. Nazarko considers improving the legislative basis for electronic evidence to be the main task, since the current legal framework lags far behind the challenges posed by digitalisation, complicating the effective use of such evidence in criminal proceedings [18].

By Law No. 3604 IX dated 23 February 2024, the Verkhovna Rada of Ukraine amended the CPC of Ukraine regarding the phased implementation of the Unified Judicial Information and Telecommunication System. The law stipulates the use of automated workflow system, recording criminal proceedings by technical means and submitting procedural documents electronically. While it does not provide a direct definition of the *electronic evidence* term, it lays the groundwork for formalising its use in criminal proceedings, in particular through the use of e-court modules and videoconferences [19].

Consequently, the provided approaches strongly emphasize that electronic data is a distinct type of evidence in criminal proceedings. Hence, its procedural status must be regulated through legislation.

The above agrees with of A.-M. Anheleniuk's findings regarding the need for regulatory consolidation and a clear conceptual framework for electronic evidence in criminal proceedings. This is because the lack of legislative definition and standardized procedure for digital data circulation results in conflicts within law application practice, which in turn lead to the risks of violation of admissibility and reliability principles. The researcher also underlines that there are blurred boundaries between the concepts of electronic medium and evidence source, requiring clear doctrinal and procedural specification [20].

Thus, a number of court decisions that we have analysed in this research paper define admissibility criteria for certain types of electronic data viewed as evidence in criminal proceedings. For instance, an automated audio recording of a conversation (using a continuously running program on the user's device) is recognized as admissible evidence; whereas the court assesses the audio recording made with the intention of capturing a conversation as inadmissible evidence due to a violation of procedural legislation requirements [21].

17 Шульга В. Правові аспекти застосування цифрових доказів у кримінальному процесі. *Діджиталізація судово-експертної науки в умовах воєнного стану* : зб. мат-лів Міжнар. наук.-практ. конф. (Харків, 08.11.2024). Харків, 2024. С. 408—410. URL: https://surl.li/czlrua (date accessed: 25.06.2025).

18 Nazarko A. E-Evidence in Ukrainian Criminal Justice: Exploring the Legal Realities and Theoretical Perspectives. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 80. Ч. 2. С. 183—188. DOI: 10.24144/2307-3322.2023.80.2.28 (date accessed: 26.06.2025).

19 Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-комунікаційної системи : Закон України від 23.02.2024 р. № 3604-IX. URL: https://zakon.rada.gov.ua/laws/show/3604-20#Text (date accessed: 26.06.2025).

20 Ангеленюк А.-М. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 79. Ч. 2. С. 214—218. DOI: 10.24144/2307-3322.2023.79.2.32 (date accessed: 25.06.2025).

21 Там само.

Based on the findings, it seems that inconsistent interpretation of electronic evidence by courts is caused by a lack of clear legal regulation, uncertainty in terminology and a failure to distinguish between the medium and source of electronic information. Admissibility of audio recordings often depends not on their technical characteristics, but on whether they were acquired in accordance with relevant procedural rules. This indicates that legal formalisation is no less important than technical credibility. Similarly, a comparable situation exists with video recordings, where the method of obtaining them plays a leading role. To ensure uniformity in law application and compliance with the principles of a fair trial, it is crucial to legally regulate the procedure for the circulation, admissibility and relevance of electronic evidence in criminal proceedings.

Peculiarities of forensic collection of electronic evidence stem from the specifics of its origin, storage and methods of transmission. Most frequently, such evidence takes the form of digital traces: *IP* addresses, *log* files, electronic correspondence, media files, or metadata relevant to criminal proceedings. They are of value to the investigation since they can ascertain facts relating to the offender, location, time and manner of a crime [22].

In European countries, particularly France, Germany, Portugal and Sweden, electronic evidence is formally equated to traditional written evidence. Simultaneously, most national laws do not contain a separate regulatory definition of the *electronic evidence* concept. Instead, they make use of scientific definitions or general procedural provisions. Despite the lack of a unified approach, EU countries are showing an intention to unify the practice of collecting, storing and exchanging digital evidence [23].

Alongside national legislation, international legal acts play a pivotal part in regulating the collection of electronic evidence. These include the European Convention on Mutual Assistance in Criminal Matters of 1959 [24], which laid down fundamental principles of international cooperation in the field of criminal justice, particularly with regard to obtaining evidence beyond national jurisdiction. The 2001 Budapest Convention on Cybercrime [25] is of particular importance in the context of investigating electronic evidence. This document was the first and remains the main international treaty intended to address issues concerning countering cybercrime (in particular, by unifying procedures for recording, collecting, storing and transmitting digital traces).

The Budapest Convention provides mechanisms for cooperation between states to ensure effective investigation of IT crimes. It also stipulates procedural tools for immediate data retention, access to and search of computer systems,

22 Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : монографія. Львів, 2022. 204 с. URL: https://surl.li/kdsnwm (date accessed: 20.07.2025).

23 Там само.

24 Європейська конвенція про взаємну допомогу у кримінальних справах : Конвенція Ради Європи від 20.04.1959 р. ; ратифік. із заяв. і застереж. Закон. України від 16.01.1998 р. № 44/98-ВР (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/995_036#Text (date accessed: 22.07.2025).

25 Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. ; ратифік. із заяв. і застереж. Закон. України від 07.09.2005 р. № 2824-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (date accessed: 22.07.2025).

extraction of information, real-time data capture, etc. This approach aims to overcome the challenges posed by the global nature of digital evidence, its vulnerability to alteration or destruction, and the complexity of transnational cooperation between law enforcement agencies in various countries. The international regulatory framework therefore introduces all the necessary conditions for the effective and lawful collection of electronic evidence during criminal proceedings, helping to overcome legal barriers associated with international cooperation.

Principal peculiarities of forensic collection of electronic evidence encompass technical complexity of its detection, the need to involve IT specialists, and the necessity to observe procedural guarantees during its recording and processing. Promptness, integrity and authenticity of electronic evidence remain the leading criteria for its admissibility in a trial.

V. Romaniuk and T. Fomina accurately note that after the full-scale invasion of Ukraine by the Russian Federation, effective fixation and legal support of evidence against collaborators, most of whom operate in the digital space, have become of paramount importance. The authors point out that the number of criminal proceedings involving collaborative activities holds a steady high level. Therefore, there is an urgent need to improve evidence-collecting methodologies. In this case, it is important to note that a substantial body of evidence is in digital form, as collaborators' activities have been recorded on social networks, messaging apps, information platforms of the occupying authorities, etc. [26]

The researchers underscored terminological ambiguity in scientific and law enforcement practice: *electronic evidence*, *digital evidence*, *electronic (digital) evidence*, *electronic display*, using the general *electronic (digital) evidence* term to refer to information that can be obtained from various electronic sources, both open (the Internet, media, social networks) and closed (messaging apps, computers, flash drives) [27]. Simultaneously, as we have already mentioned, the CPC of Ukraine does not provide for a separate concept.

The examples from practice cited by the researchers illustrate that electronic evidence is often obtained by viewing pages on social networks (Facebook, Telegram, Tik-Tok, YouTube, Viber, etc.) and suspects' mobile devices. Evidence is recorded using screenshots, screen recordings, and data copying. This allows the court to recognise such records as reliable and admissible evidence [28].

As correctly observed in this study, digital information is particularly vulnerable with regard to its evidentiary status. This is because it can be easily forged, modified or destroyed. It is precisely this characteristic that necessitates a meticulous, standardised and professional approach to its recording and storage. From M. Pashkovskyi's perspective, which is supported by other researchers in digital forensics, observing internationally recognised protocols, specifically *the Berkeley Protocol,* is cru-

26 Романюк В. В., Фоміна Т. Г. Зазнач. твір. DOI: 10.32631/vca.2024.2.25 (date accessed: 29.06.2025).

27 Там само.

28 Там само.

cial in ensuring relevance, admissibility and authenticity of such evidence [29].

Unfortunately, the researcher found that the Ukrainian pre-trial investigation authorities were not complying with the fundamental technical procedures set forth in this protocol. They predominantly create screenshots, which are the main form of visualising digital content. Concurrently, they fail to acknowledge the necessity of preserving the original *HTML* code of web pages, multimedia attachments, hidden or embedded files, metadata and *Hash* values. The above collectively enable the identification and verification of the authenticity of a digital object. As stated in the *Berkeley Protocol*, the lack of this information is a significant shortcoming in the procedure for documenting digital traces. This may cast doubt on the credibility of evidence collected during a trial [30].

Moreover, the analysed judgments often do not contain the web archiving of sources from which digital evidence was obtained. Meanwhile, utilizing special web archiving tools (e.g., means of creating captured snapshots, web resources and their development over time) is an important guarantee that the page presented did indeed look a certain way at the time of viewing and has not been altered after extracting (retrieving) data. The clear uncertainty surrounding this procedure diminishes the probative value of obtained information and poses a risk to the implementation of the adversarial principle in a court.

Thus, the considerations outlined in M. Pashkovskyi's work, logically stemming from V. Romaniuk and T. Fomin's analysis, highlight the urgent need for a regulatory and methodological rethinking of how electronic evidence is processed in modern warfare. Despite certain positive shifts in Ukrainian criminal procedural legislation (notably the recognition of computer data as documents under Art. 99 of the CPC of Ukraine [31]), detailed procedural guarantees regarding ways of collecting, recording and storing digital information are to be provided.

In this regard, incorporating international standards (in particular, *the Berkeley Protocol*) into domestic law application practice seems not only desirable but also absolutely essential. Implementing this will ensure the authenticity and reliability of electronic evidence, preventing pre-trial investigation findings from being challenged in court due to procedural violations when obtaining evidence.

Given that legislative regulation of electronic evidence in Ukraine is still in its infancy, and current criminal procedural legislation does not contain clearly formulated rules that would comprehensively define the procedure for submitting, collecting, storing and evaluating digital evidence, the pre-trial investigation stage becomes especially important in the absence of a systematic regulatory approach. The initial documentation of digital information takes place at this stage, and can be initiated by either the

29 Пашковський М. І. Зазнач. твір. С. 46. URL: https://surl.lt/wpqxyo (date accessed: 25.06.2025) ; Berkeley Protocol on Digital Open Source Investigations / Human Rights Center, Un. Nat. Human Rights Office of the High Commissioner. New York and Geneva, 2022. 102 p. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (date accessed: 25.06.2025).

30 Berkeley Protocol … . URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (date accessed: 25.06.2025).

31 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 16.07.2025).

prosecution or the defence. This determines further admissibility of such evidence in court.

R. Maliuha's studies analyse various scientific approaches to understanding the essence of the evidence collection process. Specifically, he underscores that certain researcher view it as an activity aimed at identifying, recording, seizing and preserving evidentiary data. Others focus on a broader interpretation, believing that evidence collection also encompasses examining and analysing received evidence. Some scholars argue that individual stages—discovery, search and recording—are independent stages in the overall system of evidence collection. Furthermore, there are those who believe that creating an evidentiary base covers all actions from the moment of discovering potentially valuable information to its corresponding documentation [32].

Discovering evidence is the initial stage of its collection and consists of a meticulous search for or attention to events, circumstances or physical objects that may contain information relevant to criminal proceedings. Oftentimes, such identification takes place within the framework of investigative (search) actions. R. Maliuha, based on the provisions of reflection theory, explains that evidence is in the nature of traces that remain after a criminal offence has been committed and are preserved in the material environment [33].

Collecting electronic document evidence involves identifying and properly documenting the physical medium on which it is stored, if applicable; it may also entail ensuring access to the digital environment in which relevant information is stored. This may be a server, cloud storage or an Internet resource, and accessing such resources is considered to be the process of obtaining electronic evidence. Accordingly, in the context of criminal proceedings, an investigator, inquiry officer or prosecutor may collect electronic documents through various procedural means, specifically: voluntary disclosure of such information by a participant in the proceedings, requesting required materials, temporarily accessing relevant data as a security measure, or through investigative (search) actions (e.g., inspection or search) or within the framework of covert investigative (search) activities [34].

An investigator or inquiry officer may obtain an electronic document during a search, inspection, or based on a statement or motion from a participant in the proceedings. The person must be informed of their right to voluntarily surrender documents. Even if documents are voluntarily handed over during a search, it is advisable to continue the search, as other important items may be hidden [35].

However, the CPC of Ukraine and other regulations fail to provide clear rules on the procedure for including electronic evidence, or information on the forms and content of documents confirming such procedure. Evidence may be deemed inadmissible because the way it

32 Малюга Р. В. Доказування в кримінальному процесі: проблеми визначення структурних елементів. *Наукові записки Львівського університету бізнесу та права*. 2013. Вип. 11. С. 280—283. URL: http://nbuv.gov.ua/UJRN/Nzlubp_2013_11_71 (date accessed: 16.07.2025).

33 Там само.

34 Там само.

35 Чаплинський К. О. Тактика проведення окремих слідчих дій : монографія. Дніпропетровськ, 2006. 416 с. URL: https://surl.li/wwpdti (date accessed: 20.06.2025).

was obtained or included was not specified. For instance, if case files do not include information about how the investigator obtained the photos, the court may choose to disregard the inspection record of objects (i.e., images) as a form of evidence [36].

Therefore, the process of identifying and collecting electronic evidence is characterized by a multi-level structure encompassing both technical and procedural components. The success of recording and subsequently using such evidence primarily stems from compliance with the form, method of obtaining and documentation. Simultaneously, the lack of clear procedural guidelines for attaching digital materials could result in their being declared inadmissible, which directly impedes the pre-trial investigation.

In light of this statement, one can proceed with a more comprehensive analysis regarding the peculiarities of procedural formalization of evidence, specifically documentary confirmation of its authenticity and source of origin.

Therefore, if voluntary transfer of documents is recorded exclusively in the inspection or search records, it may pose a risk of the relevant evidence being recognised as inadmissible. As for electronic documents, they should be properly included in the case file on the basis of a statement or motion submitted by a party to the proceedings, requesting the inclusion of a document stored on a physical medium. At the same time, it is advisable to record the transfer of an electronic document using video technology, especially if it is provided as part of investigative actions that require mandatory video recording (e.g., during a search or inspection).

In the context of a pre-trial investigation, a participant in criminal proceedings has the right to voluntarily provide evidence, including electronic documents, exclusively to an investigator, inquiry officer or prosecutor, and only within the framework of current criminal proceedings. This position has been upheld in judicial practice: the court of cassation supported the conclusions of the appellate court that the disc with video recordings from the store's surveillance cameras, which served as the basis for the conviction by the court of first instance, was obtained by an unauthorised official: an operative. This continued until the entry of information into the Unified Register of Pre-Trial Investigations and in breach of procedural requirements. Declaring such evidence permissible is not something that is possible in this case. Consequently, the prosecution's arguments on the legality of obtaining this evidence are groundless [37].

As V. Vapniarchuk notes, evidence may be demanded or obtained from several categories of subjects in criminal proceedings [38].

36 Вирок Ленін. райсуду м. Харкова від 01.12.2015 р. Справа № 642/6283/15-к. Провадж. № 1-кп/642/531/15 / ЄДРСР : вебсайт. URL: http://reyestr.court.gov.ua/Review/53911255 (date accessed: 20.07.2025).

37 Постанова Верховного Суду від 07.09.2019 р. Справа № 607/14707/17. Провадж. № 51-2604км19 / ЄДРСР : вебсайт. URL: http://reyestr.court.gov.ua/Review/83589933 (date accessed: 20.07.2025).

38 Вапнярчук В. В. Витребування та отримання, проведення інших процесуальних дій як способи збирання доказів у кримінальному провадженні. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. 2015. Вип. 3. Т. 3. С. 85—89. URL: https://surl.lu/slaknh (date accessed: 20.07.2025).

Categories of subjects collecting electronic evidence (according to V. Vapniarchuk)

I category	II category	III category
The parties and other participants in proceedings who submit relevant information in order to exercise their procedural rights and obligations. This allows them to shape the course and outcome of the proceedings so that they align with their own interests.	State authorities, institutions, organisations, and enterprises, including those engaged in investigative and operational actions. Legislative rules defining their legal status state that they are obliged to provide evidence in the course of criminal proceedings	Other persons, specifically those who are not participants in criminal proceedings. They may voluntarily provide evidence; however, the current legislation does not oblige them to do so: this action is more of a moral obligation

Within pre-trial investigative practice, there are cases when investigators actually draw up resolutions and forward them to relevant authorities in order to obtain needed documents. However, in practice, these resolutions are often disregarded or met with a refusal to provide the requested materials [39].

A. Kovalenko highlights certain peculiarities regarding the procedural formalization of electronic documents posted on the Internet:

1. Be sure to record technical parameters of a device used to access web resources, specifically the serial number of the service computer, name and version of the operating system, and software (browser) used by an authorised subject during an inspection.
2. Ensure that the web page is scaled to 100% to display its full content, and that all browser add-ons and plugins that could distort web page appearance are disabled.
3. Inspection record should include all multimedia materials attached to the web post and indicate the hyperlink for each one. Elements that are not related to the publication's content (e.g., web banners) do not need to be described.
4. The viewed web page must be printed using a service printer, making sure to note its serial number, brand and model in a record. This printed material is added to the record as the first appendix. All relevant multimedia files must be saved on a digital medium: a disc (the second appendix to the procedural document). As an alternative way of recording web content, the author suggests saving the page in **.html* format using a browser (and then transferring this file to the disc) [40].

39 Ухвала Київ. райсуду м. Полтави від 01.04.2024 р. Справа № 552/1823/24. Провадж. № 1-кс/552/707/24 / ЄДРСР : вебсайт. URL: https://reyestr.court.gov.ua/Review/118037105 (date accessed: 20.07.2025) ; Ухвала Яворів. райсуду Львів. обл. від 24.02.2023 р. Справа 944/1269/22. Провадж. № 1-кс/944/155/23 / Там само. URL: https://reyestr.court.gov.ua/Review/109184568 (date accessed: 20.07.2025).

40 Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України.* 2017. № 1 (88). С. 182—191. URL: https://surl.li/qulfww (date accessed: 20.07.2025).

From Ye. Khyzhniak's perspective, the main identifier of an electronic document posted on the Internet is its domain name, as well as a unique link to a specific web page containing materials applicable to criminal proceedings. The record of the web resource inspection must comprise standard document details:

- title,
- author,
- date of creation (if available),
- purpose,
- summary.

One way to secure such electronic evidence is to seize servers where it is stored. Specifically, *log* files containing information about data transfers can be obtained from Internet service providers and other owners of the relevant technical equipment [41].

Accordingly, in present-day academic writing, electronic evidence is increasingly viewed as a separate phenomenon in criminal procedure. However, Ukrainian scholars stress the need for a clear distinction between the form of recording evidence and the source of evidence.

Notably, A. Stolitnii and I. Kalancha reasonably underscore that the *electronic evidence* term should be applied exclusively as a theoretical category. This is because current legislation does not recognise electronic form as an independent source of evidence. The authors pinpoint that evidence sources—testimony, physical evidence, documents and expert findings—remain unchanged, while the electronic form merely serves as a means of documenting them within the criminal procedure [42].

Additionally, researchers focus on the dualistic nature of electronic information: its intangible nature requires mandatory recording on a physical medium to guarantee storage, transmission and corresponding procedural formalisation. Within this framework, they justifiably challenge attempts to categorise electronic evidence as a distinct group, as this would contradict the logic of criminal procedure and is an artificial phenomenon not recognised by either Ukrainian law or European practice [43].

Therefore, electronic evidence is not a distinct category of evidence. Rather, it is information recorded on an electronic medium that corresponds to one of the four legally defined sources of evidence. It ought to be viewed within the framework of procedural formalization, not in terms of substantive content.

Conclusions

Drawing upon the research conducted, the authors conclude that electronic evidence is becoming an increasingly important tool for identifying and recording circumstances of legal relevance in modern criminal proceedings. Its digital nature, dependence on technical environment, dynamism and vulnerability to change require participants in criminal proceedings not only to be technologically savvy, but also to handle such evidence in conformity with clearly stipulated procedural mechanisms.

Discovery, seizure, examination and proper formalisation of electronic evidence should be conducted taking into account forensic features of its nature, as well as evi-

41 Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право.* 2017. № 4 (58). С. 80—85. URL: https://surl.li/xdtcgp (date accessed: 25.06.2025).

42 Столітній А. В., Каланча І. Г. Зазнач. твір. DOI: 10.21564/2414-990x.146.171218 (date accessed: 25.06.2025).

43 Там само.

dence law requirements. Experience shows that failing to comply with these requirements can result in the probative value of digital information being lost, even if it is valuable to the investigation. This, in turn, puts at risk the foundational principles of adversarial proceedings and a fair trial.

Based on the analysis of scientific approaches and court decisions, it can be inferred that criminal law lacks sufficient clarity regarding the legal nature of electronic evidence. However, it is clear that such objects cannot be considered in isolation from their medium or outside of their technical context. That is why the main challenge in criminal procedure is ensuring that electronic evidence meets both proper procedural standards and technical reliability.

The study has demonstrated that electronic evidence is both a relevant and a critically important tool in criminal proceedings today. Its emergence has transformed traditional notions of evidence sources and highlighted the need to adapt procedural rules to the digital age.

It has been noted that domestic criminal procedural legislation does not yet provide comprehensive regulation for all stages of electronic evidence processing: from its discovery and recording to its evaluation and admissibility in court. The lack of a clear definition of the concept, legal status and proper procedure for including digital evidence substantially impedes law application and increases the likelihood of procedural errors.

Concurrently, global practice demonstrates well-founded approaches to resolving these issues through unifying technical standards, formalising mandatory recording procedures (specifically, web archiving, metadata preservation, hashing) and involving IT specialists in collection and analysis of digital traces.

Stemming from the above, it is proposed to consider electronic evidence not as a distinct classification group, but as a special form of recording factual data, necessitating regulatory specification. Principal conditions for efficient use of electronic evidence in criminal proceedings should be: formalisation of its legal status, development of standardized terminology, establishment of a clear procedure for obtaining, storing and including evidence, and introduction of international technical standards (in particular, *the Berkeley Protocol*).

Therefore, successful integration of electronic evidence into the national criminal justice system depends on the simultaneous improvement of legislation, methodology and technical support. This will ensure that the principles of adversarial proceedings and admissibility and relevance of evidence are upheld, thereby guaranteeing a fair trial.

Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення

Валерія Шульга, Ліна Калюжна

Проведено комплексний аналіз електронних доказів у кримінальному процесі, визначено їх місце та значення в системі доказів. Розглянуто сутність електронних доказів, їхню природу й особливості зберігання, фіксування й подальшого дослідження. Акцентовано на тому, що розвиток цифрових технологій створює нові можливості для збирання доказової інформації, але водночас спричиняє низку проблем, пов'язаних із допустимістю та автентичністю таких даних. Окреслено коло основних джерел електронних доказів, до яких належать комп'ютерні системи, мобільні пристрої, сервери, хмарні сервіси, цифрові камери відеоспостереження, електронні листування та інші об'єкти, що містять цифрову інформацію. Досліджено сучасні криміналістичні методи збирання електронних

доказів, зокрема методи ідентифікації, фіксування та вилучення інформації з носіїв цифрових даних. Окреслено етапи та процедури, яких слід дотримувати для забезпечення збереження інформації у незміненому вигляді, що є критично важливим для подальшої її допустимості в судовому процесі. Зауважено необхідність дотримання принципів цілісності, конфіденційності й достовірності під час роботи з цифровими доказами. Окрему увагу приділено процесуальному аспекту — порядку оформлення електронних доказів відповідно до вимог кримінального процесуального законодавства України. Проаналізовано чинні норми, що регулюють процедури збирання, зберігання та надання таких доказів до суду. Виявлено основні проблеми правозастосовної практики, поміж яких — недостатнє врегулювання питань щодо збереження електронних доказів, складність підтвердження їх автентичності й ризики фальсифікації. Зазначено необхідність вдосконалення законодавчої бази та запровадження єдиних стандартів роботи з електронними доказами. Сформульовано пропозиції щодо оптимізації механізмів збирання та процесуального оформлення електронних доказів, а також упровадження сучасних технічних засобів і програмного забезпечення, яке відповідає міжнародним стандартам.

Ключові слова: *електронні докази; кримінальний процес; криміналістика; цифрові технології; збирання доказів; процесуальне оформлення; інформаційна безпека; автентичність; цифрова експертиза.*

Financing

This research did not receive any specific grant from funding institutions in the public, commercial or non-commercial sectors.

Disclaimer

Founders had no role in the research design, data collection and analysis, decision to publish or manuscript preparation.

Participants

The authors have contributed solely to intellectual discussion underlying this document, case law research, writing and editing, and assume responsibility for its content and interpretation.

Declaration of Competing Interest

The authors declare no conflict of interest.

References

Anheleniuk, A.-M. (2023). Vykorystannia elektronnykh dokaziv u kryminalnomu protsesualnomu pravi Ukrainy (problemni pytannia) [The use of electronic evidence in the criminal procedural law of Ukraine (problematic issues)]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo.* Vyp. 79. Ch. 2. DOI: 10.24144/2307-3322.2023.79.2.32 [in Ukrainian].

Chaplynskyi, K. O. (2006). *Taktyka provedennia okremykh slidchykh dii* [Tactics for conducting individual investigative actions] : monohrafiia. Dnipropetrovsk. URL: https://surl.li/wwpdti [in Ukrainian].

Hutnyk, A. V., Khytra, A. Ya. (2022). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni* [Criminal procedural and forensic foundations of using electronic documents in proving] : monohrafia. Lviv. URL: https://surl.li/kdsnwm [in Ukrainian].

Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H. ta in. (2020). *Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh* [Application of electronic (digital) evidence in criminal proceedings] : metod. rek. / za zah. red. O. V. Korneika. Vyd. 2-he, dopov. Kyiv. URL: https://surli.cc/klrpaf [in Ukrainian].

Khyzhniak, Ye. C. (2017). Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen [Peculiarities of the digital document review during the investigation of

criminal offenses]. *Derzhava ta rehiony. Seriia: Pravo.* № 4 (58). URL: https://surl.li/xdtcgp [in Ukrainian].

Kovalenko, A. V. (2017). Osoblyvosti taktyky ohliadu elektronnykh dokumentiv pid chas dosudovoho rozsliduvannia posiahan na zhyttia ta zdorov'ia zhurnalista [The Features of Tactics of Inspection of Electronic Documents During the Pretrial Investigation of Infringements on the Life and Health of a Journalist]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*. № 1 (88). URL: https://surl.li/qulfww [in Ukrainian].

Maliuha, R. V. (2013). Dokazuvannia v kryminalnomu protsesi: problemy vyznachennia strukturnykh elementiv [Proving in criminal proceedings: issues in defining structural components]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava.* Vyp. 11. URL: http://nbuv.gov.ua/UJRN/Nzlubp_2013_11_71 [in Ukrainian].

Metelev, O. P. (2023). Tsyfrovi dokazy u kryminalnomu protsesi: vydova kharakterystyka [Digital evidence in criminal procedure: typological characteristic]. *Visnyk kryminalnoho sudochynstva*. № 1—2. DOI: 10.17721/2413-5372.2023.1-2/42-53 [in Ukrainian].

Muradov, V. V. (2013). Elektronni dokazy: kryminalistychnyi aspekt vykorystannia [Digital Evidence: Criminalistical Aspects of Using]. *Porivnialno-analitychne pravo.* № 3-2. URL: https://pap-journal.in.ua/wp-content/uploads/2020/09/3-2_2013.pdf [in Ukrainian].

Nazarko, A. (2023). E-Evidence in Ukrainian Criminal Justice: Exploring the Legal Realities and Theoretical Perspectives. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo.* Vyp. 80. Ch. 2. DOI: 10.24144/2307-3322.2023.80.2.28.

Pashkovskyi, M. I. (2023). Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh pro kolaboratsiinu diialnist: praktyka sudiv Odeskoi oblasti [Employing digital (electronic) evidence in criminal proceedings on collaborative activities: court practice in the Odessa region]. *Protydiia proiavam teroryzmu ta kolaboratsionizmu v umovakh viiny: stan ta perspektyvy* : matly Vseukr. kruhl. stolu (Kropyvnytskyi, 24.11.2023). Kropyvnytskyi. URL: https://surl.lt/wpqxyo [in Ukrainian].

Romaniuk, V. V., Fomina, T. H. (2024). Poriadok zbyrannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh pro kolaboratsiinu diialnist [Procedure for collecting electronic (digital) evidence in criminal proceedings concerning collaborative activities]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy*. T. 32. № 2. DOI: 10.32631/vca.2024.2.25 [in Ukrainian].

Shulha, V. (2024). Pravovi aspekty zastosuvannia tsyfrovykh dokaziv u kryminalnomu protsesi [Legal Aspects of Using Digital Evidence in Criminal Proceedings]. *Didzhytalizatsiia sudovo-ekspertnoi nauky v umovakh voiennoho stanu* : zb. mat-liv Mizhnar. nauk.-prakt. konf. (Kharkiv, 08.11.2024). Kharkiv. URL: https://surl.li/czlrua [in Ukrainian].

Skrypnyk, A. V. (2022). *Vykorystannia tsyfrovoi informatsii v kryminalnomu protsesualnomu dokazuvanni* [Use of digital information in the process of proving within criminal procedure] : monohrafiia. Kharkiv [in Ukrainian].

Stolitnii, A. V., Kalancha, I. H. (2019). Formuvannia instytutu elektronnykh dokaziv u kryminalnomu protsesi Ukrainy [Formation of the institute of electronic evidence in the criminal process of Ukraine]. *Problemy zakonnosti.* Vyp. 146. DOI: 10.21564/2414-990x.146.171218 [in Ukrainian].

Vapniarchuk, V. V. (2015). Vytrebuvannia ta otrymannia, provedennia inshykh protsesualnykh dii yak sposoby zbyrannia dokaziv u kryminalnomu provadzhenni [Requesting and Receiving, Other

Procedural Actions as a Means of Gathering Evidence in Criminal Proceedings]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia: Yurydychni nauky.* Vyp. 3. T. 3. URL: https://surl.lu/slaknh [in Ukrainian].

Shulha, V., Kaliuzhna, L. (2025). Electronic Evidence in Criminal Procedure: Methods for Its Detection, Investigation and Legal Consolidation. *Theory and Practice of Forensic Science and Criminalistics.* Issue 3 (40). P. 136—152. DOI: 10.32353/khrife.3.2025.10.