

Challenges of using digital evidence in pretrial investigations of online fraud: lessons for Kazakhstan from international practice

Nurdaulet Apsimet

Al-Farabi Kazakh National University, Kazakhstan

Yerbol Alimkulov

Al-Farabi Kazakh National University, Kazakhstan

Bakytkul Konysbay

Al-Farabi Kazakh National University, Kazakhstan

Akynkozha Zhanibekov

Mukhtar Auezov South Kazakhstan Research University, Kazakhstan

Alua Muratova

Gumilyov Eurasian National University, Kazakhstan

Date of submission: April 2025

Accepted in: November 2025

Published in: March 2026

Abstract

In the context of digital evidence, the issues of admissibility, authenticity, reliability, and compliance with procedural standards remain contentious in the legislation and judicial practice of many countries worldwide. The existing challenges in the use of digital evidence in pretrial investigations highlight conflicts between safeguarding personal data and the need for its use in investigations. These challenges are worsened by the increase in cybercrime, with online fraud ranking prominently among other forms. This paper aims to analyse current challenges related to the use of digital evidence in online fraud investigations and propose potential solutions. The above issues are examined in terms of their relevance to the legal system and regulatory framework of Kazakhstan. The findings reveal that in the current circumstances, the primary challenges in the field under study are both issues typical of conventional forensics (e.g., the absence of a court warrant or sanctions for collecting digital information, non-adherence to data retention and analysis requirements) and more recent problems (e.g., disruptions to the chain of digital evidence, the use of unlawful methods for collecting digital evidence). The modern demands of the forensics industry necessitate a thorough reassessment of approaches to training forensic investigators, with the establishment of a separate specialization.

Keywords

blockchain; cybercrime; digital data; digital evidence; digital forensics

Desafíos del uso de pruebas digitales en las investigaciones previas al juicio sobre el fraude en línea: lecciones para Kazajistán a partir de la práctica internacional

Resumen

En el contexto de las pruebas digitales, las cuestiones de admisibilidad, autenticidad, fiabilidad y cumplimiento de las normas procesales siguen siendo un tema polémico en la legislación y la práctica judicial de muchos países de todo el mundo. De los desafíos existentes en el uso de pruebas digitales en investigaciones previas al juicio, destacan los conflictos entre la protección de los datos personales y la necesidad de su uso en dichas investigaciones. Estos desafíos empeoran debido al aumento de los ciberdelitos, entre los que destaca el fraude en línea sobre otras formas. Este artículo tiene como objetivo analizar los desafíos actuales relacionados con el uso de pruebas digitales en investigaciones de fraude en línea y proponer posibles soluciones. Las cuestiones anteriores se examinan en términos de su relevancia para el sistema jurídico y el marco normativo de Kazajistán. Los hallazgos revelan que, en las circunstancias actuales, los principales desafíos en el campo en estudio son tanto problemas típicos de los análisis forenses convencionales (p. ej., ausencia de una orden judicial o sanciones para recopilar información digital, incumplimiento de los requisitos de conservación y análisis de datos) como problemas más nuevos (p. ej., interrupciones en la cadena de pruebas digitales, uso de métodos ilegales para recopilar pruebas digitales). Las demandas modernas de la industria forense requieren una reevaluación exhaustiva de los enfoques para capacitar a los investigadores forenses, así como el establecimiento de una especialización independiente.

Palabras clave

cadena de bloques; ciberdelitos; datos digitales; evidencia digital; análisis forense digital

Introduction

With the rapid digitalization of economies and social interactions, crime has also evolved, adopting new forms and methods. In recent years, cybercrime, and more broadly, online crime (from a criminal law perspective, these two concepts are often seen as complementary), has shown steady growth, while traditional types of crime have either declined or remained stable globally. This is due to the transformation (evolution) of tools and methods used to commit some traditional crimes (Murphy, 2024). As early as 2022, according to estimates from major fintech and telecom companies such as Stripe and Juniper, global losses from online payment fraud in 2020 amounted to 130 billion US dollars. Moreover, they forecast that by 2027, cumulative global losses over four years, starting in 2023 will reach approximately 340 billion US dollars (Juniper Research, 2022; Stripe, 2023). In 2024, the Global Anti-Scam Alliance (GASA), in collaboration with Feedzai, published its report on the current state of online fraud worldwide, revealing staggering data on the prevalence and impact of fraud globally. The report, based on data from various regions, highlights the substantial economic losses incurred by consumers due to online fraud. In 2024 alone, approximately

1.03 trillion US dollars were stolen worldwide, which is comparable to the annual budgets of large countries (Rogers, 2024). Despite statistical discrepancies and differing methodologies for calculating damage and classifying crimes, it is evident that the trend indicates to a steady increase in cybercrime. One of the most common crimes in the virtual space is online fraud, which includes various schemes of deception, from phishing and fraudulent online stores to complex financial manipulations involving cryptocurrencies. Online fraud (also referred to as internet fraud and cyber-enabled crime/fraud) is traditionally considered a criminal offence, as it is characterized by direct intent, a degree of public danger typical of criminal offences (crimes), and other features that distinguish online fraud from other types of wrongful actions.

The rise of cybercrime has created new challenges for criminal investigations, particularly in the collection and analysis of digital evidence (DE). The lack of standard, unified protocols for handling digital evidence complicates its admissibility in court and leads to errors in law enforcement and judicial assessments of evidence (Rakha, 2024). Effective investigation of such crimes is impossible without the use of digital evidence - data obtained from

electronic sources, including messenger platform communications, network activity logs, IP addresses, transaction information and other digital footprints. However, their use in pretrial investigations entails a range of problems related to both the technical aspects of collection and analysis and the legal issues of admissibility and reliability of such evidence. Against the backdrop of increasing cybercrime, the use of DE for investigative purposes is becoming increasingly important for many countries, including the Republic of Kazakhstan (RK). The use of evidence involves the handling of evidence for the purpose of providing proof. The criminal law doctrine in post-Soviet countries holds that the use of evidence encompasses both its examination and evaluation (Meretukov, 2015). The term “electronic evidence” began to be actively used in judicial practice after the adoption of the Federal Rules of Evidence (FRE) 1001 (Graham, 2016) in the United States, which specified the admissibility of electronic data in court. The Budapest Convention on Cybercrime has enshrined the term in international law. The widespread use of the concept in criminal investigations, including digital evidence from mobile devices and cloud services, became prevalent from 2005 to 2010. In 2019, the Committee of Ministers of the Council of Europe adopted guidelines aimed at facilitating the use of electronic evidence in civil and administrative proceedings. These guidelines cover the collection, seizure, transfer, storage and preservation of electronic evidence, and also address issues of admissibility and reliability.

Currently, online fraud is one of the most common types of cybercrime, and without electronic evidence, its investigation is practically impossible. Because fraudsters operate remotely, digital footprints are the only means of establishing their guilt and holding them accountable. In the context of pretrial investigations, the proper evaluation and management of electronic evidence is of paramount importance. Modern studies explore various aspects related to the application of digital evidence in pretrial investigations. The works in this field focus on the competence of prosecutors and investigators in the use of digital evidence (Miller, 2023) and on the collection of evidence using blockchain to detect cybercrimes (Balmiki, 2023). Some studies examine potential directions for digital transformation in pretrial investigations through the

lens of protecting individuals’ rights and legal interests (Demura *et al.*, 2020). Factors leading to the commission of internet fraud have been analysed in the Republic of Kazakhstan (Namysov, 2024). Other critical issues that have received research attention include the admissibility of digital evidence (Yeboah-Ofori & Brown, 2020), the automation of forensic examination systems for websites (Vidya *et al.*, 2022) and sources of error in digital forensics (Horsman, 2024).

The relevance of this research topic stems primarily from the need to examine challenges in personal data protection in the digital age. It is also necessary to address numerous threats to businesses and the nonprofit sector posed by the theft and leakage of commercial information and personal data. The aim of this paper was to analyse the current challenges associated with the use of digital evidence in the investigation of online fraud and to identify potential solutions.

1. Materials and methods

The documentary and analytical basis of this research includes international acts on the handling of digital evidence in pretrial investigations as well as on the collection of evidence from ICT systems (Convention on Cybercrime, 2001,¹ United Nations Convention against Cybercrime, 2024,² Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings, The Council of Europe Recommendation No. R (95) 13, Appendix, IV. Electronic evidence). The study also employed ISO/IEC standards (27037, 27042, 27043), data from analytical reports by Europol (Internet Organised Crime Threat Assessment (IOCTA) 2024) and OSCE (Stoilkovski, 2022), as well as analytical materials from legal firms and companies in the field of digital forensics (Eclipse Forensic. Breaking the Chain: Common Mistakes in Digital Evidence, etc.). The methodological foundation of the research is system analysis, which involves considering various aspects of digital evidence (DE) and their interdependencies in the context of their application in pretrial investigations. Problems related to the collection and analysis (or processing, in a broader sense) of DE were examined from two perspec-

1. The Council of Europe Convention on Cybercrime, 2001.
2. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.

tives: as indicators pointing to both the evolution of cybercrime and the evolution of forensics as a science, field of knowledge and applied activity.

Considering theoretical limitations, the work situates its analysis within Kazakhstan's national legislation, focusing on issues of digital evidence admissibility mainly through the perspective of national procedural practice. International regulations and precedents are referenced to identify global trends and approaches to managing digital evidence.

2. Results

The concepts of evidence and proof are fundamental to civil and criminal proceedings. Proof consists of gathering, verifying, evaluating evidence and using it to establish facts relevant to the case, as well as justifying the conclusions drawn from them (Vapniarchuk *et al.*, 2018). The emergence of the term "electronic (digital) evidence" has somewhat changed the perception of evidence as a material object. Digital evidence (DE), in turn, is a derivative product of certain crimes (criminal offences) with a complex taxonomy; these crimes share a common feature - they are committed using electronic equipment and typically in the internet environment. In these conditions, traditional forensics requires new skills and knowledge from specialists. Law enforcement agencies always strive to obtain as much data as possible to support any ongoing investigations. Circumventing complex security schemes incentivizes law enforcement to invest resources in knowledge and expensive equipment for advanced forensic examinations to respond to various challenges. Investigative agencies also focus their efforts and investments on identifying and exploiting security vulnerabilities to circumvent security controls and obtain digital evidence. For example, in the United States, law enforcement policy in this area aims to strengthen the role of digital forensics and expand the participation of digital forensic experts in countering cybercrime (particularly corporate cybercrime), despite numerous practical obstacles (Cybersecurity and Infrastructure Security Agency, 2022; U.S. Attorney's Office, Central District of California, 2022). Although other countries have implemented similar measures, the United States and the European Union lead in this area. In these countries, forensic science, as a component of the system for protecting and safeguarding human rights, has traditionally been of great significance (Stoilkovski,

2022). In the glossary of digital forensics, the concept of DE occupies a central place. Based on a combination of definitions, DE can be conceptualized as any information in digital form that has probative value and can be used as reliable evidence in court. According to the Council of Europe, electronic evidence means "any evidence derived from data contained in or produced by any device, the functioning of which depends on a software programme or data stored or transmitted over a computer system or network" (Committee of Ministers of the Council of Europe, 2019). In scientific sources, this definition is considered similarly. In a broader sense, electronic evidence is any probative information stored in electronic form on any type of computer device that can be used as evidence in legal proceedings (Casey, 2011; Volonino, 2003).

The problems of using digital evidence in pretrial investigations of online fraud can be conditionally divided into three main categories - technical, legal and organizational. The first category includes the complexity of extracting digital data, their mutability and instability, the lack of unified standards in digital forensics, and the difficulty of identifying the criminal due to the specific tools (instruments) used to commit a crime (electronic means and systems). The practice of criminal investigations in different countries demonstrates that digital evidence is frequently found on servers outside the country where the investigation takes place. Moreover, the information is stored in encrypted form or in data clouds, access to which is difficult. Electronic footprints can be easily forged, deleted, or altered without proper documentation, making their use in court even more challenging. Digital forensics also lacks unified standards - methods of collecting and analysing digital evidence may vary, affecting their reliability. At the same time, the use of VPNs, anonymizers, TOR networks, fake accounts, and cryptocurrencies by criminals to conceal their identity poses additional challenges to forensic investigators.

The second category - legal problems - encompasses the ambiguous status of digital evidence, as many countries have yet to enact clear regulations on their admissibility in criminal proceedings. Additionally, this category includes issues such as authenticity and reliability, as well as the absence of international mechanisms for investigative cooperation. Thus, courts may doubt the authenticity of digital evidence due to its mutability. Typically, online fraud is cross-border in nature, but the process of obtaining digital data from abroad entails bureaucratic complexities. In

addition to the aforementioned aspects, there is the problem of insufficient regulation of data collection from private sources. This problem implies potential conflicts between the protection of personal data and the necessity of its use in investigations.

The third category (conditionally titled organizational problems) refers to insufficient training of law enforcement agencies, issues of interaction with the private sector and lengthy investigation periods. The lack of expertise in cybercrime investigations and digital forensics among modern forensic investigators is a long-standing and acute issue, stemming from the specific nature of the educational programmes rooted in legal studies. Regarding the limitations of technical resources, there is a systemic opposition between “private” and “public”: the operational tools of private actors often outpace the inertia of the state. In other words, state agencies generally lag behind fraudsters in terms of technology and tools for analyzing digital footprints. In this situation, the state tends to adopt a “reactive” approach, which forces the state (represented by law enforcement agencies) to implement countermeasures. In contrast, the position of fraudsters is generally proactive. Regarding the problems of interaction with the private sector, participants in investigative actions, in one or another procedural capacity (in this case, internet companies, banks, and communication operators), may refuse to provide data or do so with delays. In conclusion, it is worth noting that the extended duration of investigations can lead to data loss or to an inability to identify offenders. Although this issue is not exclusive to online fraud, it is equally prevalent in this area as it is in cases of “traditional” offences.

The reports by Europol (2024) and the Global Anti-Scam Alliance (Singapore) (Rogers, 2024), as well as analytical data from British and American cybersecurity companies (CYBSAFE, 2024; Palatty, 2025), identify the most common types of online fraud. These include:

- Phishing - one of the most common types of cyber-crime. According to the Anti-Phishing Working Group (APWG), the monthly volume of phishing attacks worldwide was approximately 250-300 thousand in 2024;
- Financial pyramid schemes and investment fraud are the largest-scale crimes in terms of financial losses. Fake investment projects (cryptocurrency schemes, HYIPs) promise high returns, with new investors

paying the returns of earlier participants. In 2022, in the United States alone, losses from investment fraud amounted to \$3.3 billion (based on data from the FBI's Internet Crime Complaint Center) (Federal Bureau of Investigation, 2022);

- Extortion and blackmail. Extortionists threaten to publish personal data, photos, or videos, demanding money to prevent it. Criminals also use ransomware that blocks access to the victim's files until a “ransom” is paid. Theft of personal data and its resale;
- Organization and maintenance of fake online stores and services;
- Telephone fraud (especially via IP telephony, which classifies these as cyber-enabled crimes), as well as sending SMS messages containing malicious links to phishing sites;
- Cryptocurrency fraud - arguably the newest and most “technological” of all crimes related to online fraud. These crimes involve fake ICOs (initial coin offerings), pyramid schemes disguised as DeFi projects, theft of private keys, and hacking of cryptocurrency wallets. This category also includes offers for “remote (cloud) mining” (Finance Magnates, 2023).

As can be seen, online fraud is constantly evolving, and it is currently difficult to predict the “bifurcation point” at which a new evolutionary leap will occur. However, it is evident that two components will definitely be involved in this process - social engineering and technological development enhanced by the capabilities of artificial intelligence (AI). Although the latter is not yet widely cited in reports as a factor *hic et nunc*, its impact is clearly inevitable.

In light of the above, it is important to understand the criteria for admissible (legit) digital evidence. In criminal investigations of online fraud, legit digital evidence may include data from correspondence and online communications, records of telephone conversations and VoIP calls, data on financial transactions and similar information. A necessary condition is the confirmation that their collection and processing are carried out in accordance with the legislative requirements and procedures of the countries where such collection and processing occur. At the international level, these issues are partially regulated by ISO/IEC standards, such as ISO/IEC 27037, 27042 (ISO, 2012, 2015). Although these standards are essentially recommendatory documents without regulatory authority, they generally serve as the basis for preparing instructions for

digital forensics experts. An analysis of these standards can discern parameters that render digital evidence admissible for investigations and juridical proceedings. Thus, proper evidence may include:

- Data from correspondence and online communications. These are typically chats and messages on messaging platforms, correspondence on social networks, and emails (with preserved headers, metadata and delivery routes). Such data must be authenticated (e.g., through judicial requests to platforms) and must not be altered or falsified;
- Records of telephone conversations and VoIP calls (audio recordings of calls on Skype, Zoom, etc.), as well as call log files from communication providers. General requirements include the need to obtain a court warrant for access to such data, as well as to ensure confirmed sources of the recordings;
- Data on financial transactions and cryptocurrencies, e.g., bank transfers, bank statements, transactions from cryptocurrency exchanges, data on wallets and cryptocurrency addresses. As a general requirement, data must contain information about the sender and recipient. Access of competent services to such data is primarily determined by judicial decisions;
- Data on account logins (logins, IP address history of the suspect's account logins, geolocation data, cookies and metadata from websites). Such data can only be provided upon official request to internet service providers and web services, and must be in compliance with the rules of storage (analysis, processing) of the chain of custody necessary for the investigation of relevant categories of cases;
- Data from the suspect's devices obtained through physical access (files on a hard drive or flash drive, browser history, cached pages, saved passwords, auto-fill forms);
- Log files from servers and hosting platforms (records of activity on websites used to conduct fraudulent activities), data on payments on specialized platforms (e.g., PayPal) and information on domain registration and changes of ownership. Forensic experts must confirm the immutability of log files when working with them;
- Video recordings of suspects (e.g., webcam recordings, recordings of video conferences conducted during fraudulent activities, videos from ATMs or stores confirming the withdrawal of money by the fraudster). Evidence must be collected lawfully (for instance, sur-

veillance camera recordings must be obtained through a request), and it must be clear and identifiable. As in previous cases, access to such materials may require a court warrant (or a prosecutor's warrant, depending on the jurisdiction). All the above data can be used in the investigation of online fraud if they are collected legally, authenticated and not subject to manipulation. At the same time, non-compliance with procedural norms may lead the court to deem them inadmissible when considering cases.

In order to identify the main problems encountered in the collection and processing of DE, it is necessary to analyse materials from the OSCE Guidelines on Cybercrime Investigation (Stoilkovski, 2022), UNODC (United Nations Office on Drugs and Crime, 2024), Information Commissioner's Office Guidance on the use of storage and access technologies impact assessment (Information Commissioner's Office, 2024), as well as materials from private organizations specializing in digital forensics (Cyber Centaurs, 2024; Lucid Truth Technologies, 2024). In pretrial investigations of online fraud, common procedural violations include the collection of DE without a court-issued warrant, breaches in the chain of custody for DE, and insufficient authentication of DE. In addition, illegal methods of collecting DE (i.e., those that contravene established procedures) and failure to adhere to required timeframes for DE storage and analysis are also prevalent. The absence of a court warrant often arises during the seizure of digital storage devices (computers, smartphones, servers, etc.), in cases involving access to correspondence in messenger platforms, email, or cloud storage without court permission, as well as during wiretapping and internet activity monitoring without proper procedural grounds. In the United States, the case *United States v. Warshak* established a legal precedent, with the court ruling that law enforcement agencies' access to a suspect's emails without a warrant constituted a violation of the Fourth Amendment and was therefore unlawful (United States Court of Appeals, 2010).

Breaches in the chain of custody of digital evidence occur in the absence of detailed documentation on who, when and how seized, copied and analysed digital evidence, as well as in cases of non-compliance with digital forensics standards when copying data (particularly, the absence of hashing, making it impossible to verify the integrity of files). This issue is often highlighted by companies specializing in digital forensics (Belkasoft, 2024; Eclipse Forensic, 2024). In procedural terms, a breach in the chain of custody

of evidence can be identified either at the court's initiative or at the parties' request during the evidence examination stage. Present studies provide evidence that this typically occurs when the defence challenges the authenticity or integrity of digital data. If the court finds that the chain of custody has been breached, the relevant evidence may be deemed inadmissible or its probative value significantly reduced (Caianiello & Camon, 2021; IJIS Institute, 2024).

The lack of proper authentication of digital evidence implies using screenshots of correspondence on social networks or messenger platforms (as evidence) without verifying their authenticity, as well as presenting files and logs in court without proof that they have not been altered. Thus, in another case, *United States v. Vayner* (United States, 2014), the court dismissed a VKontakte page as inadmissible evidence because the prosecution failed to establish that the page definitively belonged to the defendant (VLex, 2014). The problem of employing unlawful methods to collect digital evidence generally stems from a broader issue in forensics – the use of illegal practices to obtain evidence. Although this issue is not the only one, it remains one of the most prevalent. In practice, investigative agencies may resort to installing spyware (keyloggers, trojans, etc.) without court authorization, coerce suspects into providing passwords or encryption keys without legal grounds, and collaborate with hackers or private individuals to obtain evidence illegally (TCDI, 2023). Another significant issue is the failure to comply with established protocols for the storage and analysis of digital data. Delays in analysing seized digital evidence can lead to its loss, while the absence of proper backups or the premature destruction of files before the investigation is concluded further exacerbates the problem (Information Commissioner's Office, 2024). As a result, all these errors can lead to the annulment of evidence in court, and investigators may even face charges for procedural violations.

In many jurisdictions, using digital evidence without proper judicial authorization can lead not only to the evidence's inadmissibility but also, in some cases, to the

annulment of the entire proceeding (a ground for terminating criminal proceedings). For example, Article 238 of the Spanish Organic Law of Judicial Power (LOPJ)³ provides for the invalidity of judicial actions taken in violation of fundamental procedural guarantees. Article 11.1 of the LOPJ provides that evidence obtained, directly or indirectly, in violation of fundamental rights and freedoms is null and void. Similar rules are contained in the criminal procedural laws of many other countries (in particular, the Codice di Procedura Penale of Italy,⁴ Art. 191). The Polish legislature takes a different position. The country's Code of Criminal Procedure stipulates that evidence cannot be declared inadmissible solely on the grounds that it was obtained in violation of procedural provisions or through a prohibited act.⁵ This demonstrates the increasingly close relationship between data protection, procedural legality and the admissibility of digital evidence. Regarding supranational regulation, at the international legal level, some of the main regulatory instruments for combating cybercrime and handling DE are the Council of Europe Convention on Cybercrime (Budapest Convention, 2001) and the UN Convention against Cybercrime (2024). The interaction of these two conventions is generally seen as a set of complementary regimes that lay the foundations of legal regulation and avenues for cooperation (legal, technical, and procedural). At the same time, both conventions entrust national jurisdictions with the implementation of the provisions concerning the admissibility, relevance, reliability and evaluation of DE in criminal proceedings.

Many of the previously mentioned problems regarding admissibility of DE have been noted in earlier analytical studies and institutional reports (American Bar, 2016; Goodison *et al.*, 2015). This fact indicates that the issue has become deep-seated and is likely to persist in the foreseeable future. To date, there is no clear evidence that forensic experts face difficulties with the set of technical tools or that regulatory standards inadequately describe the algorithms underlying their actions in obtaining or processing DE. This suggests that the main source of problems is the human factor – namely, the actions of forensic experts. Looking

3. ORGANIC LAW 6/1985, OF 1 JULY, ON THE JUDICIARY [online]. Available at: <https://www.legal-tools.org/doc/881df4/pdf/#:~:text=Article%20122%20of%20the%20Spanish,the%20Official%20State%20Gazette%20n%C2%BA>
4. Codice di procedura penale Testo del D.P.R. 22 settembre 1988, n. 447 [online]. Available at: <https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-di-procedura-penale>
5. USTAWA z dnia 6 czerwca 1997 r. Kodeks postępowania karnego [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-postepowania-karnego-16798685>

ahead, one might arrive at the surprising conclusion that reducing human involvement could lessen the scope of issues, with certain tasks potentially being automated (for instance, through AI techniques such as digital evidence authentication). However, under the current conditions, this scenario appears unrealistic. Forensic investigation tactics remain largely discretionary, often necessitating *ad hoc* solutions and expertise in human psychology. Forensic practice is highly context-dependent, requiring flexibility, interpretation, and adaptation to the unique circumstances of each case. While artificial intelligence may assist in identifying and prescreening evidence, the final decision regarding the admissibility, consistency and legal relevance of evidence ultimately lies with humans. Moreover, automation fails to address the critical issue of trust. The judicial system demands explicitness and clarity in decision-making. For instance, if an AI system asserts the authenticity or falsity of evidence, it is imperative to understand the rationale behind its conclusion. Unlike humans, algorithms cannot articulate their reasoning in a legally acceptable manner, which restricts their role in legal processes. Thus, while AI can serve as a valuable tool in forensics, it cannot replace human judgment at this stage.

In light of the current circumstances, the most viable solution appears to be strengthening the professional training of experts in the field (primarily criminalists and forensic investigators, and to a lesser degree, prosecutors and judges). For instance, the seminal report of the RAND Justice, a project operating under the auspices of the National Institute of Justice (the United States), focused on digital forensics in the United States. The report highlighted the critical need to train prosecutors to utilize digital evidence more effectively. It observed that many prosecutors lack a comprehensive understanding of the appropriate use and limitations of digital evidence, often leading them to request excessive amounts of data from devices – far beyond what is necessary for a case. This practice creates an unnecessary burden for digital forensic experts. In conclusion, the report recommended expanding federal training programmes to include more prosecutors, thereby improving their understanding of the types and volumes of data required as evidence in different types of cases (Goodison *et al.*, 2015).

Practising lawyers (American Bar, 2016; Fynd Academy, 2025) emphasize the educational aspect of forensics (the retraining or additional training of experts), as it is identified as a top priority in the guidelines of international organiza-

tions such as the OSCE and Interpol (Interpol, 2021; Stoilkovski, 2022). The issue of retraining criminologists in digital forensics is especially critical for countries experiencing rising levels of cybercrime, which conventional methods cannot effectively address. In particular, in Kazakhstan, by the end of 2024, approximately 17,000 cases of internet fraud were recorded (Turlybek, 2024) – a sharp 40-fold increase from around 500 cases in 2018 (Finprom, 2024).

Nevertheless, the qualifications of many specialists fall short of the requirements for working effectively with digital evidence. Common errors include improper collection and storage of evidence, the possibility of overlooking cryptocurrency transactions, and an inability to identify criminals who use tools such as Tor, VPNs or the darknet (Saniyazova *et al.*, 2024; Satbayeva *et al.*, 2024). Furthermore, Kazakhstan's legislation in this area remains underdeveloped. While there are standards for protecting personal data, clear regulations for handling digital evidence are insufficient. Furthermore, the country is not a signatory to the Budapest Convention, which hampers international cooperation.

These gaps often result in evidence being declared inadmissible in court due to procedural errors. To address these challenges, specialized training programmes should be introduced within the Ministry of Internal Affairs, Prosecutor's Office, and judicial system of the Republic of Kazakhstan. It is also essential to develop specialized regulations, such as implementing ISO standards in digital forensics and formalizing the principles of digital evidence, as well as establishing local standards for the proper handling of digital evidence.

3. Discussion

Comprehensive and reliable global data on specific issues related to violations of forensic procedures in DE acquisition and analysis (such as breaches in the chain of custody) are currently lacking. However, these issues rank among the most serious challenges in modern criminology, as highlighted by secondary sources – materials from law firms and companies specializing in digital forensics (D'Anna *et al.*, 2023; Horsman, 2024).

Modern researchers frequently argue that deviations from standard procedural protocols are the primary cause of DE processing issues (Rakha, 2024; Seo, 2024; Tosza, 2024; Ute-

pov & Zhempiisov, 2022). A growing concern among experts is the integrity of the chain of custody (De Abreu Motta, 2023; Miller & Singh, 2024; Salih & Ibrahim, 2023), particularly given the complexity of certain forensic procedures in DE operations – it is extremely challenging to strictly adhere to forensic protocols. At the same time, breaches in the chain of custody can undermine the probative value of DE. Standard methods, such as simple file copying, often fail to meet forensic requirements. Despite this, such methods are still commonly used in practice. Forensic protocols mandate the use of specialized tools (FTK Imager, Autopsy, etc.) to extract data without altering the original source (Salman *et al.*, 2023). Specialized studies have rightly emphasized that, within the EU, courts may reject evidence if it was collected in violation of the General Data Protection Regulation (GDPR) or if the procedures for obtaining it were inadequately documented (Antoliš, 2023; Wairimu *et al.*, 2024).

Other issues, such as insufficient authentication of digital evidence and noncompliance with time requirements for storing and analysing digital data, have received less attention. These are often perceived as “technical” obstacles that do not require forensic experts to acquire complex new skills in response to industry advancements (Al-E'mari *et al.*, 2024; Singh *et al.*, 2022). Meanwhile, the use of unlawful methods to obtain digital evidence is typically examined within the broader context of forensic issues (Antoliš, 2023; Li *et al.*, 2021).

Addressing crimes such as the theft of private keys and the hacking of cryptocurrency wallets requires forensic experts to possess specialized knowledge and expertise in digital forensics, blockchain technology and cryptography. Given this fundamental premise, it is evident that forensic science, as a practical discipline, must reexamine its methodological foundations for training specialists. Regarding the previously discussed integration of AI tools and their potential role in forensic techniques and strategies, this issue has not received the attention it deserves. The unique nature of forensic activities involving digital evidence demands high technical proficiency, strict adherence to procedural regulations and the use of specialized tools. A review of the methodological framework for training digital forensic experts should be considered a critical step in addressing these challenges, as well as similar issues that may emerge in the future. For many countries, including Kazakhstan, the lack of a specific term to describe professionals in this field of criminology underscores the relevance of this issue. For instance, in Russian-language literature, the term *форензик* (forensic) is increasingly used to denote this

professional field, though this may lead to confusion in the future (Mironov & Milaeva, 2024). Simultaneously, it is clear that criminology, as a scientific discipline, is undergoing a transformative phase. This is driven by the evolution of the forensic profession from a purely legal practice to a hybrid domain that combines law and computer science. This shift necessitates specialists possessing not only personal and professional qualities but also expertise in related and even unrelated fields. To train a modern forensic expert, it is essential to equip them with specific knowledge in areas such as cryptography and blockchain technology. Specifically, they must understand the principles of cryptographic key usage and storage in cryptographic wallets, as well as be familiar with symmetric and asymmetric encryption, hashing algorithms and digital signatures. Additionally, expertise in algorithms used for protecting cryptographic data, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), is crucial (Bhadarge & Parkhe, 2024; Cui & Li, 2023). To work effectively in the evolving blockchain industry, forensic experts must also have a foundational understanding of various blockchain platforms, their unique features and the use of smart contracts. Educational programmes designed to train digital forensics experts should include content aimed at enhancing professionals' ability to trace blockchain transactions, analyse blockchains and develop methodologies for detecting fraudulent or illegal transactions. Furthermore, such programmes should provide insights into anonymity-enhancing cryptocurrencies (e.g., Monero and Zcash) and their implications for investigations (Almutairi & Moulahi, 2023).

Other aspects pertain to enhancing knowledge and skills in the analysis of digital evidence. This implies the ability to use digital forensic tools and techniques to extract and analyse data such as log files, blockchain transactions and cryptographic key histories. Specialists must be proficient in employing software solutions that enable them to monitor blockchain transactions and identify connections between addresses. Additionally, it is essential for specialists to utilize cryptocurrency wallets to review transaction histories, identify suspicious activities, and detect patterns indicative of illegal actions (Ahmed & Alabi, 2024). This set of skills also includes a comprehensive understanding of cybersecurity principles, including methods for hacking cryptocurrency wallets, detecting malware (keyloggers or trojans) and analysing malicious attacks. The category conditionally titled “computer and technical skills” involves the ability to work with anonymous services and platforms that may facilitate illegal cryptocurrency transactions, as well as knowledge of

the unique characteristics of darknet marketplaces, where stolen cryptocurrencies are often traded (Anju *et al.*, 2022).

Questions related to prevention and investigation methods can be grouped into a separate category. These are closely tied to the methodological rationale for employing modern digital forensic tools. In particular, this category includes techniques for tracking cryptocurrencies (e.g., blockchain analysis to identify unusual or suspicious transactions) and evidence-gathering methods, such as retrieving information from cryptocurrency wallet addresses, obtaining transaction records, and identifying potential suspects. While these aspects align with traditional forensic tactics and procedures, the terminology in this emerging field remains underdeveloped.

Against this backdrop, it is crucial to emphasize the need to incorporate a dedicated module on legal issues into educational programmes – specifically, the legal aspects of working with cryptocurrencies and blockchain technology. The practice of experts in this field invariably involves understanding the laws and regulations governing the use of cryptocurrencies across various jurisdictions, including issues related to confidentiality, monitoring of financial transactions and cryptocurrency exchanges. Moreover, specialists must be proficient in processing court requests, working with standardized forms of appeal, and properly requesting information from exchanges, blockchain platforms and other digital services while ensuring compliance with legal requirements.

Different stages of pretrial investigations demand distinct approaches to digital evidence, ranging from collection and preservation to analysis and presentation in court. Errors at any stage can result in evidence being deemed inadmissible. Without comprehensive training of specialists based on updated methodological frameworks, even the most advanced technical improvements will remain ineffective. Furthermore, the unique nature of forensic activities involving DE requires high technical expertise, strict adherence to procedural rules and the use of specialized software and hardware tools.

Conclusions

It is evident that cybercrime continues to evolve, giving rise to new techniques and methods for committing crimes (criminal offences), and it is difficult to predict where and when the next evolutionary step will occur. Nevertheless, there is reason to believe that social engineering and tech-

nological advancements, fueled by rapid technological progress and the integration of artificial intelligence, will play a decisive role in this process. In the current context, the primary challenges in applying DE to pretrial investigations of cybercrimes, such as online fraud, encompass both traditional forensic issues and emerging complexities. Previously, non-compliance with court decisions or warrants for the collection, retention, and analysis of digital data was more prevalent. Digital forensic investigations have led to the emergence of other violations, such as breaches in the chain of custody for digital evidence, the absence of court-issued warrants or orders from competent authorities for collecting digital data, as well as the use of illegal methods to obtain DE. To date, there is no clear evidence suggesting that forensic experts face serious difficulties due to a lack of technical tools or insufficient regulatory standards outlining the procedures for acquiring and processing data. Accordingly, the primary source of error lies in the human factor – specifically, the actions and decisions of forensic experts. At the same time, the role of these experts remains indispensable, requiring flexibility, interpretation, and adaptation to the unique circumstances of each case. In this regard, the most viable solution appears to be enhancing the professional training of experts in the field (primarily criminalists and forensic investigators, and to a lesser degree, prosecutors and judges). The modern demands of the forensic sector necessitate a major overhaul of training approaches for forensic investigators, including the establishment of a separate discipline. This can be achieved by revising educational methodologies in forensics, thoroughly studying international standards for handling digital evidence (ISO/IEC 27037, 27042, 27043), gaining practical experience with certified forensic tools, and developing skills in analysing complex fraud schemes and cryptocurrency transactions. Additionally, enhancing expertise in applying artificial intelligence to criminology is crucial. Educational programs should also place greater emphasis on understanding the legal admissibility of digital evidence and the requirements of national legal frameworks governing its use.

Acknowledgments

This research was funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan within the framework of the program-targeted financing project BR27101389, “The introduction of artificial intelligence tools into the legislative process of the Republic of Kazakhstan to optimize efficiency and enhance the transparency of legislation”.

References

- AHMED, A. A.; ALABI, O. O. (2024). "Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review". *IEEE Access*, vol. 12, pp. 102219-102241. DOI: <https://doi.org/10.1109/ACCESS.2024.3429205>
- AL-E'MARI, S.; SANJALAWI, Y.; MAKHADMEH, S.; ALQUDAH, H. (2024). "Digital forensics meets blockchain: Enhancing evidence authenticity and traceability". In: *2024 2nd International Conference on Cyber Resilience (ICCR)*. Dubai: IEEE, pp. 1-6. DOI: <https://doi.org/10.1109/ICCR61006.2024.10532961>
- ALMUTAIRI, W.; MOULAH, T. (2023). "Joining federated learning to blockchain for digital forensics in IoT". *Computers*, vol. 12, no. 8, p. 157. DOI: <https://doi.org/10.3390/computers12080157>
- ALTALOX (1988). "Codice di procedura penale, Testo del D.P.R. 22 settembre 1988, n. 447". *Altalex* [online]. Available at: <https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-di-procedura-penale>
- AMERICAN BAR ASSOCIATION (2016). "Forensic Examination of Digital Devices in Civil Litigation: The Legal, Ethical and Technical Traps". *American Bar Association* [online]. Available at: https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/2016/volume-24-number-1/forensic_examination_digital_devices_civil_litigation_legal_ethical_and_technical_traps/
- ANJU, A.; KAUR, C.; KONDAPALLI, S.; HUSSAIN, M.; BEGUM, A.; HASSEN, S. M.; BOUSH, M. S. A.; BENJEED, A. O. S.; ABDALRAHEEM, M. H. O. (2022). "A mysterious and darkside of the darknet: A qualitative study". *Webology*, vol. 18, no. 4, pp. 285-294. [online]. Available at: [https://www.webology.org/data-cms/articles/20220224072305pmwebology%2018%20\(4\)%20-%2073.pdf](https://www.webology.org/data-cms/articles/20220224072305pmwebology%2018%20(4)%20-%2073.pdf)
- ANTOLIŠ, K. (2023). "The challenges of collecting digital evidence across borders". *Policija i Sigurnost*, vol. 32, no. 3, pp. 271-289. DOI: <https://doi.org/10.59245/ps.32.3.2>
- BALMIKI, V. (2023). "An evidence collection using blockchain for cybercrime detection". In: S. J. C, Varma (ed.). *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)*. Bangalore: IEEE, pp. 1-7. DOI: <https://doi.org/10.1109/GCAT59970.2023.10353259>
- BELKASOFT (2024). "Preserving chain of custody in digital forensics". *Belkasoft*, [online]. Available at: https://belkasoft.com/preserving_chain_of_custody
- BHADARGE, T.; PARKHE, D. (2024). "Comparing traditional and digital methods for detecting forged signatures in forensic analysis". *International Journal for Research in Applied Science and Engineering Technology*, vol. 12, no. 4, pp. 2073-2086. DOI: <https://doi.org/10.22214/ijraset.2024.60271>
- CAIANIELLO, M.; CAMON, A. (2021). *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*. San Giuliano Milanese: Wolters Kluwer, pp. 1-272. [online]. Available at: <https://iris.unimore.it/bitstream/11380/1230941/2/CAIANIELLO-CAMON%2C%20Digital%20forensic%20evidence.pdf>
- CASEY, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Cambridge: Academic Press.
- CYBER CENTAURS (2024). "Exposing Weaknesses in Digital Evidence for Effective Defense". *Cyber Centaurs* [online]. Available at: <https://cybercentaurs.com/blog/exposing-weaknesses-in-digital-evidence-for-effective-defense/>
- COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE (2019). "Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings". *COE* [online]. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c
- CUI, W.; LI, Y. (2023). "An improved algorithm for elliptic curve digital signature". In: *2023 42nd Chinese Control Conference (CCC)*. Tianjin: IEEE, pp. 8830-8833. DOI: <https://doi.org/10.23919/CCC58697.2023.10240757>
- CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (2022). "Combating Cyber Crime". *CISA* [online]. Available at: <https://www.cisa.gov/combating-cyber-crime>

- CYBSAFE (2024). "The Annual Cybersecurity Attitudes and Behaviors Report". *Cybsafe* [online]. Available at: <https://www.cybsafe.com/whitepapers/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-24-25/>
- D'ANNA, T.; PUNTARELLO, M.; CANNELLA, G.; SCALZO, G.; BUSCEMI, R.; ZERBO, S.; ARGO, A. (2023). "The chain of custody in the era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data". *Healthcare*, vol. 11, no. 5, p. 634. DOI: <https://doi.org/10.3390/healthcare11050634>
- DE ABREU MOTTA, A. (2023). "The importance of the chain of custody of expert evidence in digital and digitized processes in the civil sphere". *Revista Gênero e Interdisciplinaridade*, vol. 4, no. 1, pp. 458-496. DOI: <https://doi.org/10.51249/gei.v4i01.1228>
- DEMURA, M.; KLEPKA, D.; KRYTSKA, I. (2020). "Ensuring of the rights and legal interests of the person in the conditions of "digitalization" of criminal proceedings". *Law Review of Kyiv University of Law*, vol. 1, pp. 295-301. DOI: <https://doi.org/10.36695/2219-5521.1.2020.59>
- ECLIPSE FORENSIC (2024). "Breaking the Chain: Common Mistakes in Digital Evidence Handling". *Eclipse Forensics* [online]. Available at: <https://eclipseforensics.com/breaking-the-chain-common-mistakes-in-digital-evidence-handling/>
- EUROPOL (2024). "Internet Organised Crime Threat Assessment (IOCTA)". *Europol* [online]. Available at: <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>
- FEDERAL BUREAU OF INVESTIGATION (2022). "Internet Crime Report". *IC3* [online]. Available at: https://www.ic3.gov/AnnualReport/Reports/2022_ic3report.pdf
- FINANCE MAGNATES (2023). "Is Cloud Mining a Scam?". *Finance Magnates*.
- FINPROM (2024). "Losses caused by internet fraud in Kazakhstan has reached 7 billion tenge". *Finprom* [online]. Available at: <https://finprom.kz/ru/article/usherb-ot-sluchaev-internet-moshennichestva-v-kazahstane-vyros-do-7-milliardov-tenge>
- FYND ACADEMY (2025). "Chain of Custody in Cyber Security (Digital Forensics): Importance, Process, and Best Practices in 2025". *Fynd Academy*.
- GOODISON, S. E.; DAVIS, R. C.; JACKSON, B. A. (2015). "Digital evidence and the US Criminal Justice System". *RAND Corporation* [online]. Available at: <https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf>
- GRAHAM, M. H. (2016). "Handbook of federal evidence". *Miami Law* [online]. Available at: https://repository.law.miami.edu/fac_books/8/
- HORSMAN, G. (2024). "Sources of error in digital forensics". *Forensic Science International: Digital Investigation*, vol. 48, 301693. DOI: <https://doi.org/10.1016/j.fsidi.2024.301693>
- IJIS Institute (2024). *Analysis of the Law Enforcement Digital Evidence Imagery Lifecycle*. Law Enforcement Imaging Technology Task Force [online]. Available at: <https://ijis.org/wp-content/uploads/2024/05/LEITTF-Digital-Evidence-Whitepaper.pdf>
- INFORMATION COMMISSIONER'S OFFICE (2024). "Guidance on the use of storage and access technologies impact assessment - DRAFT". *ICO* [online]. Available at: <https://ico.org.uk/media/about-the-ico/impact-assessments/4032165/storage-and-access-tech-guidance-final-draft-ia-for-consultation-20241219.pdf>
- INTERPOL (2021). "Guidelines for Digital Forensics First Responders". *Interpol* [online]. Available at: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf
- ISO (2012). "ISO/IEC 27037:2012. "Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence". *ISO* [online]. Available at: <https://www.iso.org/ru/standard/44381.html>
- ISO (2015). "EN ISO/IEC 27042:2022 Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence". *ISO* [online]. Available at: <https://www.iso.org/standard/44406.html>
- JUNIPER RESEARCH (2022). "Online Payment Fraud Losses to Exceed \$343 Billion Globally Over the Next 5 Years". *Juniper* [online]. Available at: <https://www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-343bn/>

- LI, M.; LAL, C.; CONTI, M.; HU, D. (2021). "LEChain: A blockchain-based lawful evidence management scheme for digital forensics". *Future Generation Computer Systems*, vol. 115, pp. 406-420. DOI: <https://doi.org/10.1016/J.FUTURE.2020.09.038>
- LUCID TRUTH TECHNOLOGIES (2024). "The Perils of Improper Evidence Collection: Safeguarding the Integrity of Digital Forensics". *Lucid Truth Technologies* [online]. Available at: <https://lucidtruthtechnologies.com/improper-evidence-collection/>
- MERETUKOV, A. G. (2015). "Conditions for the use of evidence in procedural decisions on criminal cases". *Society and Law*, vol. 1, no. 51, pp. 187-191. [online]. Available at: <https://cyberleninka.ru/article/n/uslovie-ispolzovaniya-dokazatelstv-v-protsessualnyh-resheniyah-po-ugolovnym-delam>
- MILLER, A.; SINGH, A. (2024). "Chain of custody and evidence integrity verification using blockchain technology". In: J. du Toit, and B. van Niekerk (Eds.). *Proceedings of the 19th International Conference on Cyber Warfare and Security*, pp. 168-176. Johannesburg: Academic Conferences International Limited. DOI: <https://doi.org/10.34190/iccws.19.1.2025>
- MILLER, C. M. (2023). "A survey of prosecutors and investigators using digital evidence: A starting point". *Forensic Science International: Synergy*, vol. 6, 100296. DOI: <https://doi.org/10.1016/j.fsisyn.2022.100296>
- MIRONOV, B. A.; MILAEVA, M. Y. (2024). "Modern perspective on the concept of crime in the field of computer information. Forensic expertise as a component of criminal law regulation of anti-corruption in the Russian Federation". *Student Science Issues*, vol. 10, p. 248. SCIFF [online]. Available at: https://sciff.ru/wp-content/uploads/2024/11/Sciff_10_98-1.pdf#page=248
- MURPHY, C. (2024). "Understanding cybercrime". *EPRS* [online]. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI\(2024\)760356_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf)
- NAMYSOV, E. D. (2024). "Factors determining the commission on Internet fraud in the Republic of Kazakhstan". *Journal of Innovation in Education and Social Research*, vol. 2, no. 1, pp. 138-142 [online]. Available at: <https://journals.proindex.uz/index.php/jiesr/article/view/528>
- Official State Gazette (1985). "ORGANIC LAW 6/1985, OF 1 JULY, ON THE JUDICIARY". *Official State Gazette*, no. 157 [online]. Available at: <https://www.legal-tools.org/doc/881df4/pdf/#:~:text=Article%20122%20of%20the%20Spanish,the%20Official%20State%20Gazette%20n%C2%BA>
- PALATTY, N. J. (2025). "90+ Cyber Crime Statistics 2025: Cost, Industries and Trends". *astra* [online]. Available at: <https://www.getastra.com/blog/security-audit/cyber-crime-statistics/>
- RAKHA, N. (2024). "Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations". *Mexican Law Review*, vol. 16, no. 2, pp. 23-54. DOI: <https://doi.org/10.22201/ij.24485306e.2024.2.18892>
- ROGERS, S. (2024). "International Scammers Steal Over \$1 Trillion in 12 Months in Global State of Scams Report 2024". *GASA* [online]. Available at: <https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai>
- SALIH, K.; AND IBRAHIM, N. (2023). "CustodyChainGuardian: Blockchain of custody digital evidence preservation system". In: B. M. Sukojo (ed.). *2023 IEEE Asia-Pacific Conference on Geoscience, Electronics and Remote Sensing Technology (AGERS)*, pp. 168-175. Surabaya: IEEE. DOI: <https://doi.org/10.1109/AGERS61027.2023.10490757>
- SALMAN, M.; BANI-SLMAN, B.; ALJAIDI, M.; SALEEM, R.; ALSARHAN, A.; QASEM, M.; INJADAT, M.; IGRIED, B. (2023). "A study of forensic tools data recovery performance". In: *2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEI)*, pp. 1-6. Zarqa: IEEE. DOI: <https://doi.org/10.1109/EICEEI60672.2023.10590383>
- SANIYAZOVA, Y.; MEDIYEV, R.; SAITOVA, E.; UTEGENOVA, G.; KZYLKHOJAYEVA, A. (2024). "Advancing forensic science in Kazakhstan: The emergence and impact of digital forensics in cybercrime investigation". *Law, State and Telecommunications Review*, vol. 16, no. 2, pp. 48-68. DOI: <https://doi.org/10.26512/istr.v16i2.49190>

- SATBAYEVA A. M.; ALIMBETOVA A. P.; BEISSENBAYEVA M. T. (2024). "Cybercrime challenges: Experience of international cooperation". *Scientific and Legal Journal «Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, vol. 3, no. 78, pp. 211-221. DOI: https://doi.org/10.52026/2788-5291_2024_78_3_211
- SEO, W. (2024). "A study on electronic evidence collection methods in foreign countries and methods for granting evidence". *The Korean Association of Criminal Procedure Law*, vol. 16, no. 1, pp. 209-263. DOI: <https://doi.org/10.34222/kdps.2024.16.1.209>
- SINGH, A.; IKUESAN, R.; VENTER, H. (2022). "Secure storage model for digital forensic readiness". *IEEE Access*, vol. 10, pp. 19469-19480. DOI: <https://doi.org/10.1109/ACCESS.2022.3151403>
- STOILKOVSKI, M. (2022). "Guidelines on cybercrime investigation". OSCE [online]. Available at: <https://www.osce.org/files/f/documents/a/8/534684.pdf>
- STRIPE (2023). "Online and ecommerce fraud statistics that are predicting the future of fraud". *Stripe* [online]. Available at: <https://stripe.com/resources/more/online-and-ecommerce-fraud-statistics>
- TCDI (2023). "The Hidden Dangers of Entrusting Forensic Data Collections to Your Internal IT Team". *TCDI* [online]. Available at: <https://www.tcdi.com/the-hidden-dangers-of-entrusting-forensic-data-collections-to-your-internal-it-team/>
- TOSZA, S. (2024). "Mutual recognition by private actors in criminal justice? E-evidence regulation and service providers as the new guardians of fundamental rights". *Common Market Law Review*, vol. 61, no. 1, pp. 139-166. DOI: <https://doi.org/10.54648/cola2024005>
- TURLYBEK, S. (2024). "MVD has explained the types of fraud". *Polisia.kz*. [online]. [online]. Available at: <https://polisia.kz/ru/v-mvd-rasskazali-o-vidah-moshennichestva/>
- U.S. ATTORNEY'S OFFICE, CENTRAL DISTRICT OF CALIFORNIA (2022). "Cyber and Intellectual Property Crimes Section. Retrieved from". *Justice.gov* [online]. Available at: <https://www.justice.gov/archives/usao-cdca/cyber-and-intellectual-property-crimes-section>
- UNITED NATIONS OFFICE ON DRUGS AND CRIME (2024). "Module Series Overview". *Sherloc* [online]. Available at: <https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime.html>
- UNITED STATES COURT OF APPEALS (2010). "Appeal from the United States District Court for the Southern District of Ohio at Cincinnati". *OPN* [online]. Available at: <https://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf>
- USTAWA z dnia 6 czerwca 1997 r. "Kodeks postępowania karnego". *Wolters Kluwer* [online]. Available at: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-postepowania-karnego-16798685>
- UTEPOV, D.; ZHEMPIISOV, N. (2022). "Legal basis for collection and attachment of digital information as proof in criminal cases in the Republic of Kazakhstan". *Jurisprudence*, vol. 1, pp. 165-174. DOI: <https://doi.org/10.51788/tsul.jurisprudence.2.1.agoo5913>
- VAPNIARCHUK, V. V.; TROFYMENKO, V. M.; SHYLO, O. G.; MARYNIV, V. I. (2018). "Standards of criminal procedure evidence". *Journal of Advanced Research in Law and Economics*, vol. 9, no. 7.37, pp. 2462-2470 [online]. Available at: <https://www.cceol.com/search/article-detail?id=808866>
- VIDYA, V.; SALY, K.; BALAN, C. (2022). "Forensic acquisition and analysis of webpage". In: B. S. Anami (ed.). *2022 2nd International Conference on Intelligent Technologies (CONIT)*, pp. 1-6. Hubli: IEEE. DOI: <https://doi.org/10.1109/CONIT55038.2022.9848303>
- VLEX (2014). "United States of America, Appellee, v. Semyon Vayner, aka Sam Vayner, aka Semen, Defendant, Aliaksandr Zhylytsou, Defendant-Appellant". *VLex* [online]. Available at: <https://case-law.vlex.com/vid/united-states-v-vayner-885228839>
- VOLONINO, L. (2003). "Electronic evidence and computer forensics". *Communications of the Association for Information Systems*, vol. 12, no. 1, pp. 457-468. DOI: <https://doi.org/10.17705/ICAIS.01227>

- WAIRIMU, S.; IWAYA, L.; FRITSCH, L.; LINDSKOG, S. (2024). "On the evaluation of privacy impact assessment and privacy risk assessment methodologies: A systematic literature review". *IEEE Access*, vol. 12, pp. 19625-19650. DOI: <https://doi.org/10.1109/ACCESS.2024.3360864>
- YEBOAH-OFORI, A.; BROWN, A. D. (2020). "Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence". *Journal of Forensic, Legal and Investigative Sciences*, vol. 6, no. 1, pp. 1-8. DOI: <http://dx.doi.org/10.24966/FLIS-733X/100045>

Recommended citation

APSIMET, Nurdaulet; ALIMKULOV, Yerbol; KONYSBAY, Bakytul; ZHANIBEKOV, Akynkozha; MURATOVA, Alua (2026). "Challenges of using digital evidence in pretrial investigations of online fraud: lessons for Kazakhstan from international practice". *IDP. Internet, Law and Politics Journal*, no. 44. UOC [Accessed: dd/mm/yy]. DOI: <http://dx.doi.org/10.7238/idp.v0i44.433072>



The texts published in this journal, unless otherwise indicated, are subject to a Creative Commons Attribution No Derivative Works 3.0 Spain licence. They may be copied, distributed and broadcast provided the the author, the journal and the institution that publishes them (IDP. Revista de Internet, Derecho y Política; UOC) are cited. Derivative works are not permitted. The full licence can be consulted on <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

About the authors

Nurdaulet Apsimet

Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University, Almaty, Kazakhstan
apsimet.nurdaulet@gmail.com

Master of Legal Sciences degree. He is a doctoral student at the Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University, Almaty, Kazakhstan. His research interests are: cybercrime, internet fraud, criminal law, etc.

Yerbol Alimkulov

Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University, Almaty, Kazakhstan
erbol.alymkulov@kaznu.edu.kz

Candidate of Legal Sciences degree. He is an associate professor of the Department of Criminal Law, Criminal Procedure and Criminalistics and Deputy Dean of the Faculty of Law at the Al-Farabi Kazakh National University, Almaty, Kazakhstan. His research interests are: criminal procedure, pre-trial investigation, criminal procedure law, etc.

Bakytul Konysbay

Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Kazakhstan
b.konysbay@kaznu.edu.kz

PhD degree. She is an acting associate professor at the Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Kazakhstan. Her research interests are: financial law, banking law, customs law, etc.

Akynkozha Zhanibekov

Mukhtar Auezov South Kazakhstan Research University, Shymkent, Kazakhstan
zhan.akin@gmail.com

PhD degree. He is a professor of the Faculty of Law and Member of the Board - Vice-Rector for Research and Innovation at Mukhtar Auezov South Kazakhstan Research University, Shymkent, Kazakhstan. His research interests are: criminal procedure, evidence in criminal proceedings, advocacy, etc.

Alua Muratova

Department of Criminal Law Disciplines, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
muratova_azh@enu.kz

PhD degree. She is the head of the Department of Criminal Law Disciplines at L.N. Gumilyov Eurasian National University, Astana, Kazakhstan. Her research interests are: cybercrime, online fraud, criminal justice system, etc.