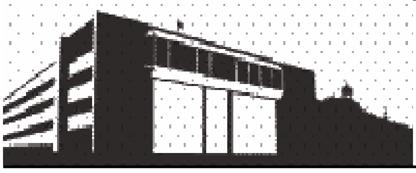

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

IRSTI 10.79.35
Scientific article

https://doi.org/10.32523/2616-6844-2024-149-4-170-185

The collection of digital traces in the investigation of online crimes

N.M. Apsimet*[1], Ye.T. Alimkulov[2], G.Zh. Duisenbayeva[3]

[1,2]Al-Farabi Kazakh National University
[3]«Q» University

(e-mail: [1]apsimet.nurdaulet@gmail.com, [2]erbol.alymkulov@kaznu.edu.kz, [3]sweet_303@mail.ru)

Abstract: The article is devoted to the study of methods of collecting digital traces in investigations of online crimes. The purpose of the study is to systematize existing approaches and evaluate their effectiveness. The scientific significance of the work lies in a comprehensive analysis of the legal, technical and ethical aspects of the use of digital traces. The article describes the stages of the data collection process, including the detection, identification, collection and preservation of information, as well as modern cyberforensis technologies. Special attention is paid to the use of artificial intelligence and machine learning methods to improve the accuracy and speed of data processing. The main results of the study demonstrate the importance of digital traces in establishing the facts of crimes. The work makes a significant contribution to the development of digital forensics, improving data analysis methods and law enforcement practice.

The article emphasizes the importance of integrating digital traces into the criminal investigation process and their role in building an evidence base. The findings obtained have practical value for professionals in the field of digital forensics and can be used to develop new approaches to the investigation of cybercrimes and improve existing techniques.

Keywords: digital traces, online crimes, cyberforensis, data analysis, investigation, collection methods, cybercrimes.

Received: 27.11.2024. Accepted: 09.12.2024. Available online: 30.12.2024.

Introduction

The growing number of online crimes, such as cyberbullying, fraud, hacking and the distribution of malicious software, highlights the relevance of studying methods for collecting digital traces in the course of their investigation. Digital traces represent important evidence that may include user data, metadata, access logs, and network footprints. They play a key role in establishing the facts of crimes and identifying suspects, as well as in subsequent court proceedings. The main purpose of this work is to study the methods of collecting and analyzing digital traces, as well as to consider their legal and ethical aspects. The objectives of the research include the classification of digital traces, the analysis of modern methods of their collection, the discussion of existing problems and limitations, as well as the prospects for the development of technologies in the field of digital forensics. A review of existing research shows that, despite significant progress in the field of cyberforensis, there remain unresolved issues related to ensuring data confidentiality, respect for citizens' rights and the legality of using the collected data in court. This work is aimed at filling these gaps and offering recommendations to improve the practice of investigating online crimes.

Research methods

The article uses an integrated approach to the study of methods for collecting and analyzing digital traces in the context of investigating online crimes. The main method includes an analysis of existing literature and scientific publications on digital forensics, which allows to systematize current knowledge about the types of digital traces, their significance and methods of analysis. Additionally, a comparative analysis of various approaches to digital data processing is carried out, including methods for analyzing network traffic, metadata and user behavior, based on the study of published studies and investigation reports.

A qualitative analysis of real cases and court cases in which digital traces played a key role is also performed. This includes examining documents related to investigations and analyzing their results, which confirms the effectiveness of the proposed methods and identifies existing limitations. The applied research methods make it possible to combine theoretical and practical analysis, providing sound conclusions and recommendations for the further development of digital forensics.

Discussion

In the modern digital world, the amount of information available about users is constantly growing. At first glance, this phenomenon may seem positive, but it also carries hidden threats. Whereas the storage of information on natural media, such as stone or papyrus, which did not present a significant risk to humans, the advent of technology has led to an increase in the digitisation of data. Unlike traditional media, digital information has a high degree of vulnerability.

Modern users, often without hesitation, leave a lot of digital traces, posting photos on social networks or just walking around the city with geolocation devices turned on. Each such trace increases the risk of becoming a victim of digital intruders. In these circumstances, it is especially important to understand the methods of protecting and preserving data. Digital footprint analysis is becoming an integral part of countering cyber threats and plays a key role in investigating online crimes. This article is devoted to the issues of collecting digital traces and their importance in the process of investigating crimes in the digital environment, as well as methods for minimizing the risks associated with information leakage.

In recent years, Kazakhstan has seen a significant increase in the number of cybercrimes, which underscores the importance of developing and applying effective investigative methods, including the collection and analysis of digital traces. According to the data provided by the Deputy Minister of Internal Affairs of Kazakhstan, the number of cybercrimes has increased more than tenfold over the past seven years. In 2024, 3,645 cases of online fraud were reported, representing an increase of 8.3% compared to the same period of the previous year. These cases account for 18% of the total number of crimes registered this year, and 43% of all fraud cases [1].

Statistics highlight the growing importance of cybercrime and the need to improve methods for collecting and analyzing digital traces. Law enforcement agencies should not only improve their technical capabilities to detect and record such traces, but also develop comprehensive approaches to their analysis to effectively identify and prevent cyber threats. Digital traces left by users and their devices on the network are becoming a key tool in investigations, helping to establish facts, identify suspects and form an evidence base. They allow us to identify patterns of behavior, connections between suspects and potential threats. In the context of the growing number of cybercrimes, the analysis of digital traces is becoming an integral part of the work of law enforcement agencies, contributing to both the detection of crimes and the prediction of offenses, which increases the effectiveness of measures to prevent cyber threats.

According to S.R. Nizayeva [2], the digital footprint is a unique set of actions of subjects in the information and telecommunications environment and the information they leave when interacting with web pages. Such traces created by individuals and legal entities are an important object of research in cybersecurity and criminology.

Nizayeva identifies two types of digital traces: active and passive. An active trail is created when a user knowingly leaves data on the Internet, for example, through posting on social networks, registering on platforms, participating in chat rooms or agreeing to use cookies. The passive footprint, on the contrary, is formed without the user's knowledge and includes automatically collected data such as IP addresses, geolocation and browsing history, used to analyze behavior and targeted advertising.

Different types of digital traces are of unique importance in investigations. The key ones include user data such as names, email addresses and phone numbers, which help identify users and understand their activity in the digital environment. Metadata, including timestamps, geolocation, and device parameters, play an important role in determining the time and location of crimes and interactions between participants.

Network traces, including web server logs, network traffic records, and IP addresses, allow to track data transmission routes and identify suspicious activity. In combination with other types of digital traces, they help to reconstruct the picture of criminal activity in the digital space.

Digital traces are also important for reconstructing the sequence of events, identifying suspects, identifying their connections, and verifying alibis. Given the rapid development of technology and the growth of cybercrime, effective collection and analysis of digital traces is becoming an essential element of investigations, requiring in-depth technical knowledge and compliance with legal and ethical standards.

The study of the types and classification of digital traces, as well as methods of their analysis and use, is an important area in the field of digital forensics. Modern approaches include the integration of traditional methods and new technologies such as artificial intelligence and machine learning, which can significantly improve the efficiency of working with digital traces and their interpretation.

Effective collection of digital traces requires adherence to a rigorous methodology that includes the identification, identification, collection and analysis of data from digital devices and network infrastructures. Digital traces can include system logs, files on hard drives, network connection records, metadata, and data that has been deleted or encrypted. These traces serve as key evidence for reconstructing events, identifying suspects and confirming their involvement in criminal activities. The main purpose of the digital footprint collection process is to ensure the integrity and authenticity of data at all stages, from their discovery and extraction to analysis and presentation in court. For this purpose, specialized methods and tools adapted to different types of data and sources are used. It is important to take into account legal and ethical standards so that the results can be used in court and do not violate human rights. The use of such approaches enables investigators not only to effectively collect and analyze digital traces, but also to guarantee their admissibility in the legal process.

The methodology for collecting digital traces includes several stages: data detection on devices (hard drives, memory), their identification and classification, as well as subsequent extraction and storage without changing the contents. For this purpose, specialized tools are used, such as predictive programs for data recovery and analysis. Important attention is paid to the protection of data from distortion and the need for technical knowledge for the correct interpretation of traces [3].

One of the elements, in gathering footprints involves examining file systems forensically to extract data from physical storage media like hard drives and other devices. Investigators use tools such as EnCase and FTK Imager to analyze the file system structure and retrieve deleted files while also examining metadata using software, like Autopsy [4]. We can use these tools to specify a timeframe for modifications, to files and reconstruct the series of computer activities performed. For instance. An examination of metadata can reveal the timing and authorship of file creation or alteration – an asset when probing instances of falsifying documents or stealing data.

Analyzing network traffic and log files plays a role, in detecting cybercrimes. By conducting network analysis, any activities can be promptly detected. Monitor the movements of potential intruders engaging in unauthorized access or DDoS attacks. This capability enables to pinpoint the origin of the threat and determine the timing of the incident vital during the initial phases of an investigation. The examination of network traffic mentioned aids, in piecing together an understanding of ongoing events. Log files keep track of all user activities and system operations to help connect any occurrences, on the network with actions taken within the system itself. This enables a sequence of events to be established to pinpoint those implement strategies to avert potential risks. The merging of information, from network traffic and log files greatly enhances the precision of investigations giving a method for analyzing events.

In inquiries often involve examining data from mobile devices as a crucial component. Mobile devices store a wealth of information, like text messages. Call records along, with app usage flags that can serve as valuable evidence. This information frequently. Validates data acquired from other channels bolstering investigators evidential groundwork.

Analyzing RAM is crucial when dealing with cyber assaults since some malware operates in memory without leaving any traces, on disks; thus, necessitating this type of examination to detect them effectively. Data retrieved from RAM aids in uncover hidden processes and network links that might remain undetected, by means.

One crucial factor involves examining data gathered from social media channels and online platforms for insights, into the relationships among individuals and their actions. This aids investigators in gaining an understanding of criminals' motives and uncovering specifics about their behavior. Integrating information from networks with findings from analyses allows for a comprehensive overview of various events, by merging diverse evidence sources into a unified investigation.

Every technique applied in the inquiry supports one another to form a strategy, for addressing cybersecurity issues and solving cases effectively. Employment of a variety of techniques and tools enables an examination of evidence resulting in successful resolution of crimes in the digital realm. Adherence to protocols and standards during data gathering and analysis guarantees their acceptance and trustworthiness in proceedings – a crucial element in ensuring fairness, in matters concerning online offenses.

The process of gathering footprints is closely tied to the series of actions that guarantee the accuracy and dependability of the information obtained. One's ability to uncover, distinguish, take control and maintain the data at every point, within the process is crucial in assuring the credibility and acceptability of proof, within a framework. It's vital to execute these stages to avoid losing data or risking its distortion or manipulation which could potentially impede the outcome [5].

In the phase of investigation called detection the focus is, on pinpointing all digital trails that could aid in the inquiry process. This phase commences by examining the network setup, equipment utilized and plausible data storage spots. Detection encompasses evaluating which gadgets and platforms might have played a role, in actions. These could include servers, desktops, smartphones, cloud storage solutions and other elements of an IT setup. Furthermore, it's crucial to take into account resources and data backups during this stage. To detect effectively one needs to comprehend the structure of the system and the specific features of the tools and programs employed within a company or a system.

Upon detection of an incident or issue arises the step of identification which entails pinpointing information or evidence pertinent, to the inquiry at hand. During this phase is when the decision is made regarding the types of data to gather; be it logs files network connections emails messages in chat apps or other forms of footprints. Identifying necessitates an evaluation of the importance of the data for the investigation as well, as an assessment of the risks linked with their retrieval. In situations, like a data breach inquiry involving data databases or a website cyberattack where web server logs are crucial for investigation purposes; legal compliance with data protection laws and authorization requirements, for accessing information are also integral aspects to consider during the identification process.

Once the important digital traces are identified and marked for extraction the next step involves extracting them to maintain their integrity and authenticity as evidence intact, throughout the process. To ensure alteration, to the data state during extraction a commonly used approach involves generating images of disks or other relevant media. Generating an image involves making a replica of all information in a systems storage without alterations even to deleted files, for future examination purposes. This method allows investigators to handle a duplicate of the data of the original version to prevent the possibility of losing evidence.

To safeguard data, against alterations or modifications effectively deploy write blockers – tools that inhibit data writing onto the device itself during examination especially crucial with tangible storage media, like hard drives or flash drives; additionally verifying data integrity using hash functions is another vital measure to undertake. Creating hash sums before and after extraction allows to make sure that the data has not been changed during copying.

The procedure for collecting and withdrawing data is regulated by the legislation of the Republic of Kazakhstan. In particular, article 253 of the Code of Criminal Procedure (CPC) describes the process of seizing specific items and documents, including digital evidence. This article requires strict rules to be followed so that the data is extracted correctly and with minimal risk of change. In addition, article 252 provides for the mandatory obtaining of judicial permission to conduct searches and seizure of data, which ensures the legality of the process [6].

Documenting all actions related to data extraction, including the tools used, timestamps, and responsible persons, plays a key role. This ensures transparency and accountability, which is necessary for the admissibility of data in court. It is also important to take into account the legal rules governing the process of data seizure, such as obtaining judicial permits to access confidential information.

The final stage, preservation, includes ensuring the safe storage of the collected data for further analysis and use in court proceedings. This stage requires the creation of reliable backups and the use of secure storage methods to prevent unauthorized access, modification or loss of data. Data retention may include the use of encryption and other security measures to ensure the security and confidentiality of the data. It is also important to comply with all legal requirements and regulations regarding the storage of digital evidence, such as requirements for the storage of personal data or compliance with the rules for handling confidential information. Proper data retention ensures their suitability for use in court proceedings and protects the rights of all parties involved.

In accordance with Article 221 of the CPC of the Republic of Kazakhstan [6], seized items and data recognized as material evidence must be stored in compliance with all procedural requirements. This includes inspection, documentation and transfer to safe custody, which guarantees their safety and suitability for use in court. Article 97 also includes security protocols that can be used to control data access this is crucial, for safeguarding information. Maintaining data integrity ensures its admissibility in legal proceedings and safeguards the interests of all stakeholders, by reducing the chances of unauthorized access and data breaches.

Properly executing each step of gathering data – starting from discovery, to storage – not guarantees the accuracy and dependability of the gathered evidence but also ensures its acceptability in legal proceedings. It plays a role, in investigating and bringing to justice individuals engaged in criminal activities online.

Collectin digital footprints involves more, than using techniques and tools; it also involves taking into account technicalities along with legal and ethical factors throughout to maintain the legality and trustworthiness of the gathered data, for potential court use and safeguard the rights of all involved in the inquiry.

Utilizing technologies is crucial, in the data collection process to guarantee information extraction while avoiding any potential data tampering or alteration risks. For instance employing write blockers when handling drives helps maintain the data integrity by preventing any modifications. Additionally generating checksums using hash functions like MD5 or SHA256 enables the verification of data immutability, at processing stages. When dealing with deleted information data retrieval specialists and specialized tools are essential to ensure recovery of data is possible while maintaining transparency, for potential court cases by thoroughly documenting each step of the data handling process.

Legal considerations are just as important, as the aspects when dealing with data collections. It's crucial to ensure that any gathered digital information follows data protection laws and international guidelines – especially if the data is being moved between countries. This involves securing permissions to access private data in a way that ensures its validity in legal proceedings. Neglect of these requirements could result in evidence being deemed inadmissible and creating hurdles in the process.

Ethical considerations are intertwined with obligations when it comes to safeguarding individuals' privacy rights. Investigators must ensure intrusion into lives by acquiring only pertinent data tied to the ongoing criminal probe. Adhering to ethical norms safeguards citizens' rights and bolsters trust, in law enforcement entities, from the eye.

Ensuring adherence to technical guidelines as well as legal and ethical principles is crucial for effectively gathering and processing digital evidence. Next comes the analysis phase of the gathered data which's vital in uncovering crucial details related to the crime. Analytical techniques used vary based on the type of data and investigative goals such, as behavior analysis, network traffic examination and metadata scrutiny to gather evidence for legal proceedings.

The utilization of intelligence (AI) and machine learning (ML) in criminological analysis methods marks a significant advancement, in combating cybercrime by automating the examination of vast data sets to expedite anomaly detection and enhance result accuracy and dependability.

Artificial intelligence and machine learning offer benefits, in automating the examination of traces while cutting down on time and lessening the necessity for manual input from experts. As data volumes continue to soar and cyber threats multiply rapidly the conventional analysis approaches demand resources and time to handle data effectively. In times machine learning methods, like neural networks and random forests have gained widespread adoption in the field of digital forensics. These algorithms help automate the data analysis process and enhance the precision of anomaly detection – an aspect, in warding off cyber attacks. For instance, utilizing networks to scrutinize log files allows for speedy identification of suspicious activities while employing random forest methods aids in spotting intricate patterns signaling fraudulent behavior. In comparison AI algorithms excel at executing this task effectively enabling responses, to new security risks. Utilizing learning methods to examine log records instantly enables the detection of irregularities, in network activity – a crucial measure, in thwart in possible cyber breaches or data breaches [7].

One of the benefits is its capability to spot patterns and irregularities, in vast data sets that might be overlooked with conventional methods. When it comes to scrutinizing network traffic containing billions of records AI algorithms can pinpoint patterns, like data flow directions or uncommon sequences of events that could signal malicious behavior. Neural network powered tools and clustering algorithms are already extensively employed in live data analysis to greatly enhance the chances of detecting threats.

Machine learning techniques enable algorithms to learn from data to enhance their capabilities, in fields like criminology for anticipating future events accurately and efficiently by recognizing trends and foresee potential cyber threats based on historical patterns of attacks. This plays a key role, in forecasting and preventing potential risks as machine learning algorithms can study past incidents to pinpoint common traits and unique characteristics of attacks thus aiding in the formulation of improved security measures. However, when predicting criminal behavior, it is important to take into account not only digital footprints, but also other risk factors such as low self-control, the influence of the criminal environment, and socio-economic conditions [8]. The implementation of algorithms can greatly cut down on the time it takes to address emergencies and lessen potential harm.

The effectiveness of AI and machine learning also stems from their capacity to adjust to evolving circumstances and emerging risks. Cyber attackers are consistently enhancing their strategies. Devisin methods to breach defenses. Machine learning techniques offer the required flexibility and adaptability enabling models to be regularly upgraded and trained with data. This enhances their resilience against shifts, in intruders behaviors. This is especially important in an environment where cyberattack methods are becoming more complex and sophisticated, requiring continuous updating and adaptation of security systems.

The use of AI and ML in real-world scenarios of digital forensics has already proven its effectiveness. For example, AI-based algorithms are actively used to analyze network traffic in order to identify anomalies and prevent attacks. ML methods also play an important role, which facilitate the creation to create behavioral models of normal network activity, automatically identifying any deviations indicating possible threats.

In addition, AI and ML play a key role in the investigation of cybercrimes, such as hacks or data leaks. Automatic analysis of data from devices and network logs enables investigators to quickly identify the source of the attack and determine the method of penetration of intruders. This significantly speeds up the investigation process and increases the likelihood of bringing the perpetrators to justice. In the financial sector and e-commerce, AI and ML are also actively used to detect fraudulent transactions. For example, machine learning algorithms can analyze transaction data in real time and identify suspicious activity, preventing financial losses and protecting users from fraud.

The effectiveness of AI and ML in digital forensics has been confirmed by a number of international studies. These technologies not only speed up data analysis processes, but also significantly increase the accuracy of threat detection and prediction of cyber attacks.

The use of digital traces in real investigations confirms their importance for the successful detection of complex cybercrimes. For example, during the international investigation of financial fraud called «JuicyFields», the analysis of digital traces turned out to be a key factor in tracking the movement of funds through several banking institutions and identifying links between participants in a criminal network. Coordinated actions by law enforcement agencies from different countries, with the support of Europol, led to the arrests and liquidation of the criminal network, which became possible thanks to in-depth data analysis [9].

With the constant growth of data volumes and the increasing complexity of cybercriminal methods, the use of AI and ML is becoming a necessary tool for successful investigations and cybersecurity.

The development of AI and ML, playing a key role in adapting to new threats, lays the foundation for a more effective and comprehensive approach to the investigation of digital crimes. In combination with traditional methods such as behavioral analysis, network traffic analysis and metadata, these technologies allow investigators not only to automate the data processing process, but also to significantly deepen their understanding of the actions of intruders. The integrated use of these methods helps not only to accelerate the analysis of digital traces, but also to identify key evidence that is critical for the successful detection of crimes and ensuring fairness in law enforcement practice.

The analysis and interpretation of digital traces, as the final stages in the investigation of online crimes, provide investigators with the opportunity not only to reconstruct the sequence of events, but also to collect the necessary evidence for a trial. Practical examples of the use of digital traces in criminal cases demonstrate their importance in establishing facts and confirming the guilt of suspects. Every year, digital traces play an increasingly important role in law enforcement practice, helping to solve both cybercrimes and traditional criminal cases using digital technologies.

One of the most striking examples of the use of digital traces in the investigation of cybercrimes, such as hacks and attacks on information systems, is the analysis of network traffic to identify the sources of attacks. For example, investigators often use methods such as full packet capture and log analysis to track suspicious connections. These methods allow to identify abnormal patterns in network traffic that may indicate the use of stolen credentials or other types of unauthorized access.

One of the most striking examples of the use of digital traces in the investigation of cybercrimes is the attack on Ukrainian government institutions, known as NotPetya in 2017. In this case, the attackers used malware to compromise the systems, launching an attack from a popular Ukrainian tax website. This has led to the infection of computer systems in various countries, including the USA, Great Britain and Germany. Analysis of network traffic and data packets played a key role in identifying the source of the attack and identifying the routes of the virus. Network analysis allowed the researchers to track the command servers, which helped stop the further spread of the virus and localize the damage [10].

This approach, as shown by real cases, allows not only to stop attacks, but also to use the digital traces obtained as evidence in court, which greatly facilitates the process of bringing charges and proving the guilt of intruders.

Digital traces are actively used in financial crime investigations around the world, and international practice shows how important digital forensics technologies are for uncovering complex fraudulent schemes. One example is the case of United States v. Ganias [11], where digital forensics was used to analyze electronic correspondence and financial documents that linked the accused to the illegal actions of his clients. This case showed how the seized digital data can be used to identify fraudulent schemes and establish the guilt of the accused. Another example concerns fraud using cryptocurrency. According to the U.S. Department of Justice, more than $112 million has been seized related to fraudulent investment platforms, where digital traces such as blockchain transaction records have become a major source of evidence. These records allowed investigators to trace the movement of funds, which helped to uncover a complex financial scheme and identify those responsible for the crime [12].

Global practice also demonstrates the importance of digital forensics in cases involving identity theft and tax fraud. In one case reviewed by the U.S. Internal Revenue Service (IRS), digital traces helped expose a criminal network that stole more than $6 million. Investigators used forged documents and digital correspondence to gather evidence and further prosecute [13].

These instances demonstrate the increasing significance of footprints, in investigations by equipping investigators with resources to accurately pinpoint perpetrators and uphold justice standards. Leveraging traces to establish facts and evidence helps construct an evidentiary foundation crucial in legal proceedings for ensuring a just trial while safeguard rights of everyone involved in the process. However this analysis of traces encounters challenges and constraints despite its critical role and efficacy, in modern investigations of cybercrimes. These issues can make it more challenging to determine facts and evidence accurately. Could impact the acceptance of data, in proceedings too. It's crucial to recognize these constraints to enhance analysis techniques and reduce the dangers linked with using information, in law enforcement activities.

A significant challenge lies in preserving the reliability and genuineness of the information gathered through means during its collection and analysis phase to maintain its credibility and safeguard it against manipulation or tampering attempts that could render it unacceptable, as evidence in proceedings ensuring data integrity necessitates employing specific techniques like hashing algorithms and encryption methods while controlling access, to the information [14]. However, with these precautions, in place there is no assurance, against all potential dangers particularly when assailants possess considerable technical prowess to tamper with information.

One other critical issue involves the evolving technologies and tactics used for hiding data that pose obstacles for investigators to overcome. Recent advancements, like encryption techniques, steganography practices and the utilization of networks greatly increase the complexity of retrieving and examining information. Malicious actors are employing tools that enable them to conceal their activities and minimize their footprints within systems. For instance, by utilizing steganography individuals are able to embed information within types of files (such as images or videos) making it almost undetectable, through analysis methods. This makes it difficult to detect illegal data and requires the use of specialized tools to identify them [15].

Legal norms related to the protection of personal data and information security play a key role in the process of collecting digital traces. These laws impose restrictions on the amount and nature of data that can be collected as part of an investigation. In the same case about United States v. Ganias [11], special attention was paid to the volume of seizure of digital evidence. As part of this case, investigators confiscated much more data than was necessary for a specific investigation, which called into question the permissibility of such widespread seizures in digital forensics. In particular, the problem of the seizure of data that is not relevant to the case and their storage for a long time was discussed, which may violate the rights of citizens and cast doubt on the legality of using such evidence in court. This case highlights the need to limit the amount of data collected, following the principles of minimization and focus when collecting digital traces. Different jurisdictions have different legal requirements, which creates difficulties for international investigations, especially when access to data is required from foreign servers. Obtaining judicial permits to access private information can slow down the process and limit the capabilities of investigators, which can negatively affect the efficiency of the investigation. Moreover, non-compliance with legal norms can lead to the recognition of evidence as inadmissible in court, which jeopardizes the success of the entire case. These legal complexities are closely related to the ethical issues that inevitably arise when dealing with digital traces. Digital data analysis often involves personal information, which requires special attention to privacy and citizens' rights. Investigators are required to minimize interference with privacy by collecting only the data that is necessary for the investigation, so as not to violate ethical standards. Not abiding by these guidelines can not just hinder the investigation. Also shake the trust of the public in law enforcement operations. A situation that can have effects, on public safety.

In addition, one of the significant problems is the management of large amounts of data and the complexity of their analysis. Modern digital investigations often involve working with large amounts of data that need to be analyzed quickly and accurately. This requires the use of high-performance computing power and advanced analytical tools such as machine learning and artificial intelligence to automate analysis processes. However, even with the use of such technologies, there is a risk of errors or false positives, which can lead to incorrect conclusions and compromise of evidence.

These challenges and limitations highlight the need for continuous improvement of methods and tools for analyzing digital traces, as well as the development of a legal and ethical framework for their use. Overcoming these challenges requires cooperation between law enforcement agencies, information technology experts and legislators to ensure the effective and legitimate use of digital data in the fight against crime.

Conclusion

This research showed how crucial it is to take an approach when gathering and examining footprints in online criminal investigations. The rise, in cybercrimes like scams and hacking underscores the need to enhance techniques for forensics. The study reviewed methods, for analyzing information and highlighted the benefits of using artificial intelligence and machine learning technologies to enhance threat identification accuracy amidst the growing volume of data.

Methods, like examining network traffic and log files remain crucial in pinpointing the origins of attacks while leveraging AI and ML offers a chance to automate the analysis of data sets, for anomaly detection and reducing human error – a significant advantage when dealing with intricate and ever evolving cyber threats.

However, the successful application of these methods requires strict adherence to legal and ethical standards so that the results can be acceptable in court proceedings. An important area of further research is the development of approaches that will ensure not only technical accuracy, but also the legality of using the collected data in international investigations.

The practical significance of the analysis lies in recommendations for improving existing methods of working with digital traces and the use of advanced technologies, which can significantly increase the efficiency of law enforcement agencies and reduce the response time to cyber threats. Further development of digital forensics methods and deeper integration of modern technologies will ensure higher accuracy of threat forecasting and improvement of law enforcement practice in the digital world.

The contribution of the authors

Apsimet N. – the author for correspondence prepared the main content of the article, summarized previous research by the topic.

Alimkulov Ye. – prepared the materials of the legal practice and the conclusion of the research.

Duisenbayeva G. – prepared the introduction and methodology of article, translated the references, abstract and information about the authors of the article.

References

1. Количество киберпреступлений в Казахстане выросло в 10 раз, 04.03.2024 – URL: https://inbusiness.kz/ru/last/kolichestvo-kiberprestuplenij-v-kazahstane-vyroslo-v-10-raz (дата обращения: 27.03.2024).

2. Низаевой С.Р. Цифровые следы. Виды, перспективы использования в целях раскрытия и расследования преступлений // Государственная служба и кадры. – 2020. – №4. – С. 189-190. doi:10.24411/2312-0444-2020-10225.

3. С.В. Петраков, М.А. Гудкова, Д.П. Бащук, А.А. Тимофеев, Д.Н. Пигильдин, И.С. Бедеров, Д.О. Сорокин, А.В. Пытайло. Сбор и анализ цифровых следов преступления: практическое пособие. – СПб: Санкт-Петербургская академия Следственного комитета, 2023. – 98 с.

4. Carrier B. File System Forensic Analysis. – Boston: Addison-Wesley Professional, 2005. – 382 c.

5. Jeff Darrington. The Phases of the Digital Forensics Investigation Process, 01.06.2023 – URL: https://graylog.org/post/the-phases-of-the-digital-forensics-investigation-process/ (Accessed: 21.11.2023).

6. Criminal Procedure Code of the Republic of Kazakhstan. The Code of the Republic of Kazakhstan dated July 4, 2014 No. 231.– URL: https://adilet.zan.kz/eng/docs/K1400000231 (Accessed: 02.10.2023).

7. Md. Fazley Rafy. Artificial Intelligence in Cyber Security. Preprint, January 2024 – URL: https://www.researchgate.net/publication/377235308_Artificial_Intelligence_in_Cyber_Security (Accessed: 14.02.2024).

8. Muratova A., Zhanibekov A., Aryn A., Nurmaganbet Y., Turgumbayev Ye., Kevin M. Beaver. What Separates Offenders Who are Not Victimized from Offenders Who are Victimized? Results from a Nationally Representative Sample of Males and Females//Victims & Offenders. – 2024. – №19(4). – P. 513-530. DOI: 10.1080/15564886.2023.2263849

9. 9 arrests in EUR 645 million JuicyFields investment scam case, 12.04.2024 – URL: https://www.europol.europa.eu/media-press/newsroom/news/9-arrests-in-eur-645-million-juicyfields-investment-scam-case (Accessed: 15.04.2024).

10. The 7 Biggest Government Cyberattacks since 2011.– URL: https://swivelsecure.com/solutions/government/top-cyber-attacks/ (Accessed: 06.12.2023).

11. United States v. Ganias and the Case for Selective Seizures of Digital Evidence, 04.10.2016 – URL: https://www.brennancenter.org/our-work/analysis-opinion/united-states-v-ganias-and-case-selective-seizures-digital-evidence (Accessed: 24.10.2023).

12. Justice Department Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, 03.04.2023 –URL: https://www.justice.gov/opa/pr/justice-department-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes (Accessed: 24.10.2023).

13. Three individuals sentenced for roles in fraud and identity theft ring that stole over $6 million in government funds, 12.01.2024 –URL: https://www.irs.gov/compliance/criminal-investigation/three-individuals-sentenced-for-roles-in-fraud-and-identity-theft-ring-that-stole-over-6-million-in-government-funds (Accessed: 05.02.2024).

14. Бисалиев М.С., Шакиров К.Н. Цифровые следы как фактор безопасности оборота персональных данных в сети Интернет //Вестник Евразийского национального университета имени Л.Н. Гумилева. Серия: Право. – 2023. – №142(1). – С. 81-98. https://doi.org/10.32523/2616-6844-2023-142-1-81-98

15. Зиновьева Н.С. К вопросу о месте криптографии и стеганографии в криминалистической науке// Гуманитарные, социально-экономические и общественные науки. – 2019. – №2. – С. 87-89.

Н.М. Әпсімет*[1], Е.Т. Алимкулов[2], Г.Ж. Дүйсенбаева[3]

[1,2]әл-Фараби атындағы Қазақ Ұлттық университеті

[3]«Q» University

(e-mail: [1]apsimet.nurdaulet@gmail.com, [2]erbol.alymkulov@kaznu.edu.kz, [3]sweet_303@mail.ru)

Онлайн қылмыстарды тергеу кезінде цифрлық іздерді жинау

Аңдатпа: Мақала онлайн қылмыстарды тергеуде цифрлық іздерді жинау әдістерін зерттеуге арналған. Зерттеудің мақсаты – қолданыстағы тәсілдерді жүйелеу және олардың тиімділігін бағалау. Жұмыстың ғылыми маңыздылығы цифрлық іздерді қолданудың құқықтық, техникалық және этикалық аспектілерін жан-жақты талдауда жатыр. Мақалада деректерді жинау процесінің кезеңдері, соның ішінде ақпаратты табу, анықтау, жинау және сақтау, сондай-ақ заманауи киберфорензика технологиялары сипатталған. Деректерді өңдеудің дәлдігі мен жылдамдығын жақсарту үшін жасанды интеллект пен машиналық оқыту әдістерін қолдануға ерекше назар аударылады. Зерттеудің негізгі нәтижелері қылмыс фактілерін анықтауда цифрлық іздердің маңыздылығын көрсетеді. Жұмыс деректерді талдау әдістері мен құқық қолдану практикасын жетілдіре отырып, цифрлық криминалистиканың дамуына айтарлықтай үлес қосады.

Мақалада цифрлық іздерді қылмыстық тергеу процесінде интеграциялаудың маңыздылығы және олардың дәлелдемелік базаны құрудағы рөлі аталып өтілді. Алынған нәтижелер цифрлық криминалистика саласындағы мамандар үшін практикалық құндылыққа ие және киберқылмыстарды тергеудің жаңа тәсілдерін әзірлеуге және қолданыстағы әдістемелерді жақсартуға пайдаланылуы мүмкін.

Түйін сөздер: цифрлық іздер, онлайн қылмыстар, киберфорензика, деректерді талдау, тергеу, жинау әдістері, киберқылмыс.

Н.М.Апсимет*[1], Е.Т. Алимкулов[2], Г.Ж. Дүйсенбаева[3]

[1,2]Казахский Национальный университет имени аль-Фараби

[3]«Q» University

(e-mail: [1]apsimet.nurdaulet@gmail.com, [2]erbol.alymkulov@kaznu.edu.kz, [3]sweet_303@mail.ru)

Сбор цифровых следов при расследовании онлайн-преступлений

Аннотация: Статья посвящена исследованию методов сбора цифровых следов в расследованиях онлайн-преступлений. Целью исследования является систематизация существующих подходов и оценка их эффективности. Научная значимость работы заключается в комплексном анализе юридических, технических и этических аспектов использования цифровых следов. В статье описаны этапы процесса сбора данных, включая обнаружение, идентификацию, сбор и сохранение информации, а также современные технологии киберфорензики. Особое внимание уделено использованию методов искусственного интеллекта и машинного обучения для повышения точности и скорости обработки данных. Основные результаты исследования демонстрируют важность цифровых следов в установлении фактов преступлений. Работа вносит значительный вклад в развитие цифровой криминалистики, улучшая методы анализа данных и правоприменительную практику.

Статья подчеркивает важность интеграции цифровых следов в процесс уголовного расследования и их роль в построении доказательной базы. Полученные результаты имеют практическую ценность для специалистов в области цифровой криминалистики и могут быть использованы для разработки новых подходов к расследованию киберпреступлений и улучшению существующих методик.

Ключевые слова: цифровые следы, онлайн-преступления, киберфорензика, анализ данных, расследование, методы сбора, киберпреступления.

References

1. Kolichestvo kiberprestuplenij v Kazahstane vyroslo v 10 raz [The number of cybercrimes in Kazakhstan has increased 10 times]. Available at: https://inbusiness.kz/ru/last/kolichestvo-kiberprestuplenij-v-kazahstane-vyroslo-v-10-raz ((data obrashcheniya: 27.03.2024). [in Russian]

2. Nizaevoj S.R. Cifrovye sledy. Vidy, perspektivy ispol'zovanija v celjah raskrytija i rassledovanija prestuplenij [Digital traces. Types and prospects of use for the purpose of disclosure and investigation of crimes] // Gosudarstvennaja sluzhba i kadry [Public service and personnel]. 4. 189-190(2020), doi:10.24411/2312-0444-2020-10225. [in Russian]

3. S.V. Petrakov, M.A. Gudkova, D.P. Bashhuk, A.A. Timofeev, D.N. Pigil'din, I.S. Bederov, D.O. Sorokin, A.V. Pytajlo. Sbor i analiz cifrovyh sledov prestuplenija: prakticheskoe posobie [Collecting and analyzing digital traces of crime: a practical guide]. (St. Petersburg, 2023. 98 p.) [in Russian]

4. Carrier B. File System Forensic Analysis. – Boston: Addison-Wesley Professional, 2005. – 382 c.

5. Jeff Darrington. The Phases of the Digital Forensics Investigation Process. Available at: https://graylog.org/post/the-phases-of-the-digital-forensics-investigation-process/ (accessed: 21.11.2023).

6. Criminal Procedure Code of the Republic of Kazakhstan. The Code of the Republic of Kazakhstan dated July 4, 2014 No. 231. Available at: https://adilet.zan.kz/eng/docs/K1400000231 (accessed: 02.10.2023).

7. Md. Fazley Rafy. Artificial Intelligence in Cyber Security. Preprint. Available at:https://www.researchgate.net/publication/377235308_Artificial_Intelligence_in_Cyber_Security (accessed: 14.02.2024).

8. Muratova A., Zhanibekov A., Aryn A., Nurmaganbet Y., Turgumbayev Ye., Kevin M. Beaver. What Separates Offenders Who are Not Victimized from Offenders Who are Victimized? Results from a Nationally Representative Sample of Males and Females//Victims & Offenders. – 2024. – №19(4). – P. 513-530. DOI: 10.1080/15564886.2023.2263849

9. 9 arrests in EUR 645 million JuicyFields investment scam case. Available at: https://www.europol.europa.eu/media-press/newsroom/news/9-arrests-in-eur-645-million-juicyfields-investment-scam-case (accessed: 15.04.2024).

10. The 7 Biggest Government Cyberattacks since 2011. Available at: https://swivelsecure.com/solutions/government/top-cyber-attacks/ (accessed 06.12.2023).

11. United States v. Ganias and the Case for Selective Seizures of Digital Evidence. Available at: https://www.brennancenter.org/our-work/analysis-opinion/united-states-v-ganias-and-case-selective-seizures-digital-evidence (accessed: 24.10.2023).

12. Justice Department Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes. Available at: https://www.justice.gov/opa/pr/justice-department-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes (accessed: 24.10.2023).

13. Three individuals sentenced for roles in fraud and identity theft ring that stole over $6 million in government funds. Available at: https://www.irs.gov/compliance/criminal-investigation/three-individuals-sentenced-for-roles-in-fraud-and-identity-theft-ring-that-stole-over-6-million-in-government-funds (accessed: 05.02.2024).

14. Bisaliev M.S., Shakirov K.N. Cifrovye sledy kak faktor bezopasnosti oborota personal'nyh dannyh v seti Internet [Digital footprints as a factor in the security of personal data turnover on the Internet] Vestnik

Evrazijskogo nacional'nogo universiteta imeni L.N. Gumileva. Serija: Pravo [Bulletin of the L.N. Gumilev Eurasian National University. Series: Law]. 142(1). 81-98(2023), https://doi.org/10.32523/2616-6844-2023-142-1-81-98. [in Russian]

15. Zinov'eva N.S. K voprosu o meste kriptografii i steganografii v kriminalisticheskoj nauke [On the question of the place of cryptography and steganography in forensic science] // Gumanitarnye, social'no-jekonomicheskie i obshhestvennye nauki [Humanities, socio-economic and social sciences]. 2. 87-89(2019). [in Russian]

Information about the authors:

Әпсімет Н.М. – хат-хабар үшін автор, докторант, қылмыстық құқық, қылмыстық іс жүргізу және криминалистика кафедрасы, заң факультеті, Әл-Фараби атындағы Қазақ ұлттық университеті, әл-Фараби даңғылы 71, 050000, Алматы, Қазақстан

Алимкулов Е.Т. – заң ғылымдарының кандидаты, доцент, қылмыстық құқық, қылмыстық іс жүргізу және криминалистика кафедрасы, заң факультеті, әл-Фараби атындағы Қазақ Ұлттық университеті, әл-Фараби даңғылы 71, 050000, Алматы, Қазақстан

Дүйсенбаева Г.Ж. – «Құқық» академиялық мектебінің аға оқытушысы, «Q» University, Байзаков көш. 125/185050000, Алматы, Қазақстан.

Апсимет Н.М. – автор для корреспонденции, докторант, кафедра уголовного права, уголовного процесса и криминалистики, Казахский национальный университет имени аль-Фараби, 71, 05000, пр. аль-Фараби, 71, 050000, Алматы, Казахстан.

Алимкулов Е.Т. – кандидат юридичесих наук, доцент, кафедра уголовного права, уголовного процесса и криминалистики, юридический факультет, Казахский национальный университет имени аль-Фараби, пр. аль-Фараби, 71, 050000, Алматы, Казахстан.

Дүйсенбаева Г.Ж. – старший преподаватель Академической школы «Право», «Q» University, ул. Байзакова 125/185, 050000, Алматы, Казахстан.

Apsimet N. – the author for correspondence, doctoral student, department of criminal law, criminal procedure and criminalistics, faculty of law, Al-Farabi Kazakh National University, al-Farabi ave. 71, 050000, Almaty, Kazakhstan

Alimkulov Y. – candidate of law, associate professor, department of criminal law, criminal procedure and criminalistics, faculty of law, Al-Farabi Kazakh National University, al-Farabi ave. 71, 050000, Almaty, Kazakhstan

Duisenbayeva G. – senior lecturer, Academic School «Law», «Q» University, Baizakov str. 125/185, 050000, Almaty, Kazakhstan.