UDC 343.16
DOI: 10.56215/naia-herald/3.2023.48

Electronic evidence as a means of proof during the pillage investigation

Yevheniia Murzo*
Adjunct
National Academy of Internal Affairs
03035, 1 Solomyanska Sq., Kyiv, Ukraine
https://orcid.org/0009-0000-4409-0560

Viktoriia Halchenko
Adjunct
National Academy of Internal Affairs
03035, 1 Solomyanska Sq., Kyiv, Ukraine
https://orcid.org/0009-0000-7164-2949

■ **Abstract.** The electronic evidence has become one of the key components of criminal investigations. The use of digital evidence allows investigating not only criminal offences against the property, environment, etc., but also offences committed during the war and invasion. Since the beginning of the large-scale invasion of Ukraine, the number of pillage cases, which became known from open sources of information, has increased. The purpose of this study was to investigate the problematic issues of using digital evidence in the pillage investigation. The methodological basis was general scientific methods of cognition, namely, scientific abstraction, deduction and induction, extrapolation, and logical generalisation. The paper examines pillage among other war crimes in the context of determining the concept, composition of a crime, and the admissibility of digital evidence during the pillage investigation of this crime. The urgency of solving problematic aspects related to the pillage investigation, primarily in the context of a full-scale war in Ukraine, is substantiated. The pillage is separated from other crimes against property committed under martial law or a state of emergency. The problems of terminology are considered and approaches to the qualification of criminal offences committed under martial law, including shortcomings in law-making, are outlined. It is proposed to amend the Criminal Procedure Code of Ukraine, defining the requirements for electronic evidence during the investigation of pillage. The practical significance of the study lies in the fact that such tools can be used for further research on the use of the digital evidence as a means of proof in the pillage investigation, as part of the development and improvement of legislation in this area

■ **Keywords:** digital criminalistics; information sources; digitalisation; criminal offence; war crimes; martial law

■ **Suggested Citation:**
Murzo, Ye., & Halchenko, V. (2023). Electronic evidence as a means of proof during the pillage investigation. *Scientific Journal of the National Academy of Internal Affairs,* 28(3), 48-57. doi: 10.56215/naia-herald/3.2023.48.

■ *Corresponding author

■ Received: 03.06.2023; Revised: 02.09.2023; Accepted: 26.09.2023

Introduction

The hostilities on the territory of Ukraine have shown how important electronic tools for searching and collecting information are for investigating criminal offences. One of the types of such criminal offences is pillage. In this situation, the entire legal system of Ukraine is faced with new challenges that need to be solved by forensic means. To establish the fact of pillage, it is necessary to collect, investigate and submit evidentiary information to the court. In the process of proof, electronic evidence is of great importance, which can be recorded by technical means.

The use of electronic evidence has become increasingly important in the pillage investigation, as modern technologies and the digital environment have a significant impact on crimes of this nature. Attackers can leave traces in the form of electronic data on computers or mobile devices, such as: text messages, email, photos, videos, social networks, etc. Law enforcement agencies can analyse this data to get important information about the crime and possible persons involved in it. Many places where the pillage takes place are equipped with video surveillance systems. Video recordings can serve as the important evidence, revealing the crimes and identifying intruders by their appearance or movements. The correct use of the electronic evidence can significantly increase the effectiveness of the investigation and help to identify and bring to justice the perpetrators of pillage.

The problems of this topic are the specifics of pillage, the existing traces of this offence, the features of identifying the perpetrator, the insufficient use of technical means, etc. In addition, under martial law, it becomes more difficult to collect and record evidence. One of the new areas of forensics, digital forensics, is gaining importance. This industry allows developing effective tools for investigating criminal offences, especially those committed under martial law, the occupation of territories, or armed conflicts, when there is a limited access to the scene of an accident or when it is impossible to get there at all.

O. Predmestnikov *et al.* (2023) expressed concern that Ukraine, having been at war for more than a year, does not use all available means of the protection, including non-ratification of the Rome Statute of the International Criminal Court, which makes it difficult to implement some of the decisions of this international body. S. Depauw (2018) analysed the role of digital evidence in criminal cases in European Union countries, drawing attention to the collection of electronic evidence, in particular content data, for criminal justice in Europe. K. Latysh (2022) investigated the use of digital forensics during the war. The researcher proposed requirements for digital evidence and considered all the aspects of martial law.

H. Mamedov (2022) found out how digital forensics and electronic evidence were used to record traces of war crimes in Bucha. Satellite images were able to prove the involvement of Russian servicemen in the killing of civilians and that mass graves appeared during the occupation. O. Yanovska (2022) highlighted the fact that the procedure for collecting and recording electronic evidence must necessarily involve a computer technology specialist. According to the recommendations developed by the National Academy of Internal Affairs, computer technology specialists can help an investigator identify, collect and record the necessary electronic evidence. In addition, a significant amount of information is located on the internet, which can potentially, under certain conditions, be used as evidence of military and other criminal offences (Latysh, 2022).

Therefore, the purpose of this study was to investigate the possibilities of electronic evidence in the investigation of criminal offences related to pillage during the martial law.

Materials and Methods

The study used a complex of general scientific and special methods. These include, in particular, methods of formal logic, namely synthesis, analysis, deduction, induction, abstraction, and analogy. With the help of these methods, the content of the issues under study was clarified in detail in order to deepen their understanding. In particular, it was possible to establish the essence of the concept of "pillage" and other related issues. The concept of pillage and its interpretation were studied using the Criminal Code of Ukraine. In particular, the issue of the admissibility of electronic evidence in the pillage investigation in various research papers was investigated. The paper considered the state of use of electronic evidence in criminal proceedings in foreign countries. In addition, research in the legal sciences should be based on three components. Legislative and regulatory – requires selecting, studying, and analysing all laws and regulations in the field of criminal law. The second component is the practical component. It is necessary to investigate the practice of using electronic evidence in the criminal offences related to pillage. In the third, it is also important to investigate theoretically and analyse scientific sources that raised the issue of the electronic evidence, and pillage during the war.

The descriptive and analytical method allowed interpreting legal categories, formulating definitions, and outlining the procedure for collecting the electronic evidence during the pillage investigation. The comparative legal method was used in the comparison of concepts and scientific research, the opinions of researchers on the concept of digital evidence, their belonging and admissibility, and was also used in the analysis of the current Criminal Procedure Code

and other legislative acts. Due to this method, a distinction was made between pillage and other crimes against property committed during martial law.

This method helped to classify and identify the features of the subject under study, to develop mechanisms for determining the admissibility of electronic evidence during the investigation of pillage. The specific sociological method allowed studying the opinions and views of researchers on the issues under study, allowed identifying and solving some practical and theoretical problems, and formulating recommendations for improving legislation in the field of admissibility of electronic evidence. The statistical method was used to summarise the results of studying the materials of criminal proceedings on the investigation of war crimes, in particular, pillage during martial law, and to substantiate the theoretical provisions of the work with statistical data. They have been collected on the number of war crimes since the start of the full-scale invasion and the percentage of crimes related to pillage was determined. The methods of forecasting and modelling were used to develop proposals for improving certain provisions of the legislation.

The methodology of using electronic (digital) evidence in the investigation of pillage under the martial law includes a set of procedures, principles, techniques, and methods of research in this area. It is based on a dialectical method of cognition of phenomena and processes, the main principles of which are consistency and complexity.

Results

The pillage is often referred to in the media as the open or secret theft of property by a person during a war. However, according to the legislation, theft of private homes, premises, vehicles, shop premises, etc. is not the pillage. The Criminal Code of Ukraine (hereinafter – CC) defines pillage as a military criminal offence, that is, it can only be committed by military personnel. According to Article 432 of the CC, pillage is the theft of things on the battlefield that belong to the dead or wounded[1]. Article 432 of the CC defines two clear criteria for qualifying pillage as a criminal offence. Firstly, there is a clear location for the commission of this crime – a theft of property on the battlefield (that is, the area where military operations are being conducted or once conducted, and this also includes the area that is under fire from military equipment). Secondly, the theft of personal belongings that are located near the dead or wounded. This applies to personal belongings, not those that can be used in future to conduct hostilities. Therefore, this offence applies only to military personnel, not civilians, and only if it is committed on the battlefield. When certain illegal actions are aimed at seizing things for the purpose of their own profit without the above-mentioned circumstances, then they cannot qualify as the pillage and relate to other criminal offences. Thus, it is inappropriate to apply the concept of "pillage" to persons who have committed a criminal offence under the martial law, but not on the battlefield and are not military personnel (Table 1).

Table 1. Differentiation between the concepts of "pillage" and "theft"

Pillage	Theft
Concept: Theft of items on the battlefield that belong to the dead or wounded (Article 432 of the Criminal Code) **Subject:** Serviceman **Place of commission:** Battlefield **Subject:** Private property of the wounded or killed persons	**Concept:** Secret theft of property (Article 185 of the Criminal Code)[2] **Subject:** Natural person of sound mind who has committed a criminal offence **Place of commission**: Any locality **Subject:** Private property, military supplies, firearms, etc.

Source: developed by the authors

The use of electronic evidence can be an important tool in the pillage investigation. The electronic evidence is information in electronic form that contains data on circumstances relevant to the case: electronic documents (text documents, graphic images, plans, photographs, video and sound recordings, etc.); websites; text, multimedia and voice messages; metadata, databases, etc., in electronic form. Such data can be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, and other places where data is stored in the electronic form (including on the Internet) (Sabadin, 2021).

The Office of the Prosecutor General is the main body that has taken over the coordination of

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[2] Ibidem, 2001.

war crimes investigations since Russia's invasion of Ukraine. As of December 2022, prosecutors recorded 62,128 war crimes, including 60,387 (97.20%) violations of the laws and customs of war – Article 438 of the CC[1], in which 135 persons were served with a notice of suspicion. The rest is propaganda of war, genocide, waging aggressive war, sabotage, propaganda, pillage, and other crimes (About registered criminal..., 2022).

The main types of electronic evidence in the investigation of pillage can be:

1. Video and photo evidence: videos and photo recordings can show the facts of pillage, show the persons involved in the crime, or record other details. Such evidence can be obtained from surveillance cameras, mobile devices of witnesses, or social networks.

2. Electronic communications: email, social media messages, SMS messages, and other forms of electronic communication may contain important information about criminals, their accomplices, or their plans.

3. Online footprints: pillage can have an electronic footprint in the form of activity on websites, forums, social networks, etc. Such data can provide important information about the actions and motives of criminals.

For the successful use of the electronic evidence in the pillage investigation, it is necessary to carry out a proper procedure for collecting, analysing and preserving evidence so that it remains complete and reliable. The decision of the Joint Chamber of the Criminal Court of Cassation of the Supreme Court of 29.03.2021 in case No. 554/5090/16-k (proceedings No. 51-1878kmo21)[2] explained how the electronic evidence is evaluated and whether different versions of the same electronic document are considered admissible. According to the Law of Ukraine "On Electronic Documents and Electronic Document Management"[3], if an electronic document is stored on several electronic media, then each of these copies is considered original, and only the content of the electronic document is important, and not the medium on which it is stored (Sabadin, 2021).

With the help of effective digital forensics tools, the investigation of war crimes becomes much more effective, especially in war conditions, when there is often no access to the crime scene (Kostenko, 2019). Moreover, the Internet contains a large amount of information that can potentially be used as evidence of military criminal offences. The task of law enforcement agencies is to obtain this data stored on electronic media, which acts as a source of criminally significant information (Okpara *et al.,* 2023).

The main digital forensics tools that can help in pillage investigations are:

- analysis of satellite images;
- geolocation tag analysis;
- examination of publicly available video and photographic materials provided to the investigation;
- use of special software for image processing and analysis;
- monitoring of telephone conversations and email correspondence;
- use of a face recognition system and search for them in special databases (in Ukraine, the Clearview AI application for face recognition is used to identify criminals and the dead).

Notably, obtaining evidence from open sources of information is something new for the Ukrainian legal system. When searching for and recording such information, it can only become the electronic evidence under certain conditions. The Law of Ukraine "On Amendments to the Criminal Procedural Code of Ukraine and the Law of Ukraine "On Electronic Communications" on Improving the Effectiveness of Pre-Trial Investigation "On Hot Pursuit" and Countering Cyberattacks" changed the legal regulation of the use of digital evidence[4]. One of the changes was that the specialist received the right to provide explanations, consultations, and references. The current Criminal Procedure Code of Ukraine and the above-mentioned law do not describe the requirements that such a certificate must meet. It can be concluded that it will refer to documents as a source of evidence.

In addition, this law defined the possibility of taking readings from technical devices and means that have the function of photo and video recording from a person who is the owner or owner of such means or devices, in order to clarify the necessary circumstances of the case. Taking readings from these technical devices is carried out based on a decision of the investigator or prosecutor and, if necessary, an appropriate specialist is involved. This resolution must contain the following data: the number and name of the criminal proceedings, information about the owner of technical devices, the period of time for which readings from technical means should be taken. Analysing judicial practice, it can be concluded

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Resolution of the Joint Chamber of the Criminal Court of Cassation of the Supreme Court No. 554/5090/16-K. (2021, March). Retrieved from https://verdictum.ligazakon.net/document/96074938.
[3] Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management". (2003, March). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15#Text.
[4] Law of Ukraine No. 2137-IX "On Amendments to the Criminal Procedural Code of Ukraine and the Law of Ukraine "On Electronic Communications" on Improving the Effectiveness of Pre-Trial Investigation "On Hot Pursuit" and Countering Cyberattacks". (2022, March). Retrieved from https://zakon.rada.gov.ua/laws/show/2137-20#Text.

that the main sources of information about the perpetrators and organisers of criminal offences under martial law are mobile phones, laptops, tablets, photo and video cameras, social networks, e-mailboxes, search engines, etc. (Stefaniv, 2022).

One of the key problems of the investigation of war crimes in Ukraine is that the main provisions of the criminal procedure legislation regarding the regulation of the definition of digital evidence and the procedure for its collection, use, and examination in criminal proceedings do not meet the conditions of the present (Fil & Khoynatska, 2022). Therefore, considering current challenges, it is necessary to make additions and changes to Chapter 4 of the Criminal Procedure Code[1], which should provide for the definition of the electronic evidence and its source. It is also necessary to determine the criteria for the ownership and admissibility of electronic evidence. In addition, the procedure for detecting, searching, recording, seizing and storing electronic evidence during investigative actions needs to be regulated.

The cybersecurity strategy of Ukraine, which was approved by Presidential Decree No. 447/202 of August 26, 2021, determined that for strengthening the state in the field of cybersecurity, the legal settlement of the problem of electronic (digital) evidence is one of the key conditions[2]. These changes will improve the effectiveness of law enforcement officers' use of electronic databases and cyberspace in general for the purpose of comprehensive and impartial investigation of criminal offences committed during the martial law and pillage in particular (Shepitko & Shepitko, 2021).

Given the process of Ukraine's integration into the European Union, the experience of these countries in the use of the electronic evidence is important. Therefore, the Council of Europe has provided "Guidelines on electronic evidence" that describe in detail the process of obtaining and processing digital evidence. It also covers the basic principles that should be followed when collecting and processing digital evidence (Gisel *et al.,* 2020). These include: legality, appropriate training, data integrity, specialised support, and a control log. Considering these principles and the above research, the following basic requirements for electronic (digital) evidence can be proposed (Tosza, 2020).

Firstly, the information and data contained on electronic media should directly relate to the circumstances of the relevant criminal offence that is being investigated. Secondly, in order to the data to be truly reliable and authentic, it is necessary to carry out an appropriate verification procedure for these data. One of the most common and recommended is the Dublin Core Metadata Element Set. According to this document, a set of fifteen "core" elements is used. To describe resources, recipients, or developers of digital data must record the following once about digital information: author, reach, creator, date, description, format, identifier, language, publisher, relationship, copyright, source, subject, title, and type (Dublin Core metadata..., 1999). Special programmes and applications can be used to automatically capture metadata. For example, the "eyeWitness to Atrocities" camera app can be used, which allows capturing videos and photos with built-in metadata that cannot be changed later. This metadata shows where and when the photo and video material was taken and whether it was changed. These photos and videos are stored in the app's secure gallery, where they cannot be edited (Cerbo, 2021). Thirdly, digital evidence must have a tangible expression, i.e., be recorded on a technical medium (phone, flash drive, computer, hard disk, etc.). These media can be attached to the materials of criminal proceedings and then reproduced in the appropriate process. It is very important to determine the source of origin of such material and establish the video recording process.

By collecting information from open sources (social networks, news sites, blogs, etc.), it is possible to review photos and videos of pillage incidents. After the examination, the investigator should appoint a forensic portrait examination or an examination of photo, video, and sound recordings to identify the person who committed a criminal offence by voice, face, etc. (Riekkinen, 2019). To avoid any traces of editing or alteration of photo, video and audio recordings, a computer forensic examination should be appointed. In order to find out the value of the object of the encroachment, it is necessary to appoint a commodity expert examination. Things that are the subject of pillage can only be those objects of the material world in respect of which civil rights and obligations arise and which are related to ensuring the sphere of the private life of a person. These items may include watches, wedding rings, pendants, etc. (Lasaka, 2023).

Thus, one of the most important procedures in criminal proceedings related to the investigation of pillage is to conduct the above-mentioned examinations. The electronic evidence plays an important role in the modern justice, especially in the context of Ukraine's integration into the European Union. To ensure the reliability and authenticity of this evidence, it is important to follow principles that include legality, appropriate training, data integrity, specialised support, and the use of metadata. Such evidence

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defense Council of Ukraine Dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text.

must have a tangible form on electronic media and be properly documented for use in court proceedings.

Discussion

Ye.O. Murzo (2023) investigates the specifics of the appointment and conduct of certain types of forensic examinations in the pillage investigation, divides electronic documents into several categories: 1) electronic documents contained on physical media; 2) electronic documents posted on the Internet; 3) electronic documents contained in special cloud services for storing information. K. Latysh (2022) studied digital forensics during the war. In particular, the researcher concluded that due to the rapid digitalisation, the role of digital forensics in the investigation of criminal offences has significantly increased. The global pandemic, frequent cyber-attacks, armed aggression, and information warfare have exacerbated the need to develop digital forensics. Generally accepted forensic scientific and technical means should be updated in accordance with the needs of the modern world, but at the same time, they should consider the requirements of the current criminal procedure legislation and international standards. This is especially true for the evidence that has been obtained and collected from publicly available sources, such as the Internet.

The authors of this study agree with this opinion, since digital forensics tools have helped to investigate pillage much more effectively. Digital forensics is of great importance in the investigation of pillage, as digital traces can provide valuable information about the crime and the persons involved (Wang & Liu, 2019). Digital forensics can include analysing social media, communication records, email, mobile phones, and other digital traces that can help identify looters (Marcello, 2015). Analysing these tracks can help identify how looters operate, their communities, and information about possible targets and plans. Criminologists can recover lost or deleted data from digital devices such as computers, mobile phones, or storage media (Abraha, 2020).

This may include recovering photos, videos, messages, or other digital evidence that can be used to identify individuals involved in pillage or establish their actions. They can also analyse network traffic passing through digital networks to identify pillage-related abuses. The use of computer vision and artificial intelligence algorithms allows forensic scientists to analyse photos and videos from surveillance cameras or mobile devices to detect pillage (Chan & Magotiaux, 2021). These tools help digital forensic investigators collect, analyse, and interpret digital data related to pillage. The use of these tools helps to collect independent, objective, and convincing evidence that can be used in legal proceedings to bring looters to justice. Thus, digital forensics plays an important role in pillage investigations, helping to identify perpetrators and establish the truth (Lewulis, 2021).

O. Predmestnikov *et al.* (2023) in their study concluded that Ukraine, which has been at war for more than a year, does not use all possible and available methods of protection. In particular, the attention was drawn to the fact that Ukraine has not ratified the Rome Statute of the International Criminal Court yet, which makes it difficult to implement some decisions of this international body. The study also established that the identification of pillage by legal scholars with a theft, robbery, or plunder is conditioned by the fact that the title of the law that increased liability for certain types of property crimes refers to the increase in liability for pillage, while the content of the law increases liability not only for this type of crime. In the course of this study, the issue of the qualification of pillage was highlighted. In order to bring real criminals to justice for a criminal offence committed, it is important to collect an evidence base, since pillage can only be committed on the battlefield.

S. Depauw (2018) investigated the role and significance of digital evidence in criminal proceedings in the European Union. This paper was intended to analyse recent developments in the collection of the electronic evidence, or rather content data, for criminal justice purposes in Europe. Firstly, a brief historical review of the EU's actions in the context of judicial cooperation in criminal matters (both in general and in relation to evidence) was conducted. Secondly, electronic evidence itself and legislation in its current form were discussed, followed by an assessment of the actions taken by both the Council of Europe and the European Union to overcome the difficulties faced by both public (law enforcement agencies) and private actors (service providers). The study evaluates the extent to which current discussions and proposals can be considered a step forward in light of technological and judicial reality.

T. Khashashneh *et al.* (2022) compared the powers of a criminal judge to evaluate digital evidence in the laws of Jordan, Egypt, and France. The interest enjoyed by digital (electronic) evidence has become great compared to other types of evidence. In fact, this is due to the spread of the use of digital information technologies, the role of which has increased with the introduction of the Internet and computers in various spheres of life. Thus, the problem with this study was that the virtual environment became a hotbed for a number of criminals, who are called information criminals. The crimes they commit are in a virtual environment. Several findings and recommendations have been made in this study, the most important of which is that digital (electronic) evidence is the best evidence to prove virtual crimes, as

it depends on the environment in which the criminal offence was committed. Hence, the interest in this type of evidence began, since the proof of a virtual crime is not limited to digital (electronic) evidence, because it can be proved by traditional methods of proof, such as: testimony, confession, etc.

J. Kancauskiene (2019) investigated the computer expertise and electronic evidence in Lithuanian criminal proceedings. Lithuanian Code of Criminal Procedure[1] first of all, regulates the receipt of electronic data, complementing the requirements of laws such as the Criminal Intelligence Act, the Police Activities Act and the Financial Crime Investigation Service, but not limited to them. Data are usually obtained in the manner prescribed by both the Criminal Intelligence Act and other laws prior to the start of a pre-trial investigation. After the opening of a pre-trial investigation, evidence is collected exclusively in accordance with the Code of Criminal Procedure[2]. The courts are particularly attentive to checking whether the evidence collected in accordance with the Law on Criminal Intelligence was obtained legally. The requirement to obtain evidence in accordance with the procedure established by law is closely related to the requirement to obtain evidence legally. Judges are obliged to carefully assess whether the evidence was obtained legally, i.e., whether the rules for obtaining evidence established by law were followed.

M. Rojszczak (2022) investigated cooperation in the field of the electronic evidence in criminal cases from the perspective of the European Union (EU). For several years, there has been a debate among EU member states about the need to regulate cross-border access to electronic data used as evidence in criminal proceedings, and how best to do this. The existing model of cooperation, based mainly on bilateral agreements, seems to be dysfunctional and is perceived by many as an obstacle to effectively combating the growth of cross-border crime. In response, work has begun on several new legal mechanisms, the main of which is the draft regulation on electronic evidence from the European Commission and the proposal to expand the convention on cybercrime, which has been in force for almost 20 years, with an additional new protocol. The United States has proposed its own model of cooperation, which follows from the CLOUD Law. This paper discusses the current state of affairs and the expected form of future regulations – in terms of both facilitating law enforcement cooperation and clarifying the obligations imposed on digital service providers.

Overall, digital forensics has become an important tool in the investigation of pillage and other crimes in the modern world. It allows the collection, analysis, and interpretation of digital data, in particular, electronic documents and other digital traces, which can be used to identify criminals and obtain reliable evidence in court proceedings. This is especially relevant in the face of modern challenges, such as: digital threats, information warfare, and rapid digitalisation. Updating and developing digital forensics tools are a necessity to ensure effective investigation and establishment of truth in the modern world.

Conclusions

This paper investigated the use of electronic evidence as a means of proof in the investigation of pillage. It is important to ensure the proper preservation of electronic evidence, as it can be used in court proceedings. This includes properly storing metadata, a chain of custody, and ensuring that it is inaccessible to third parties. The electronic evidence can be examined to confirm its authenticity and integrity. It is important to work with relevant security services, such as the police, intelligence or military, to ensure that electronic evidence is properly collected and processed. This will help to ensure the legal aspect of the pillage investigation.

In the course of the study, the requirements that electronic evidence must meet in a pillage investigation were put forward. Firstly, the electronic evidence must relate to a specific offence. Secondly, it is necessary to properly verify the evidence received. Thirdly, digital evidence must be tangible, i.e., it must be recorded on a specific technical medium (phone, computer, flash drive, etc.). It is described that proof of pillage requires the collection and presentation of convincing evidence confirming the existence of this crime. The reliable evidence and its adequate presentation will help ensure a fair investigation and the prosecution of all perpetrators. Collecting evidence of pillage on the battlefield can be difficult and cause some difficulties. Reports from people who have witnessed or suffered pillage can be an important source of information. These testimonies may be collected from civilians, military personnel, or journalists who were on the battlefield.

It is reasonable that official documents, such as police statements, medical records, or reports from human rights organisations, may contain information about cases of pillage on the battlefield. If the evidence of pillage is collected, it is important to contact the competent authorities, such as: the police, human rights organisations or international bodies, to transfer the collected information and evidence for further investigation and possible prosecution of those responsible. It is determined that international observers or missions aimed at verifying compliance

[1] Code of Criminal Procedure of Lithuania. (2002, March). Retrieved from https://www.wipo.int/wipolex/en/legislation/details/8195.
[2] Ibidem, 2002.

with human rights and international norms can work in conflict zones. Their reports and research may contain information about pillage and human rights violations on the battlefield. Notably, it is important to collect this evidence, verify its reliability and authenticity, and transfer it to the relevant authorities of the incriminated country or international organisations that have competence in investigating and bringing to justice the relevant persons.

The issue of using electronic evidence in the investigation of pillage is almost not considered by foreign researchers. The investigation of pillage may require cooperation between countries and international organisations. In the future, it is necessary to develop new norms of the international law aimed at countering pillage and punishing criminals. International legal structures may be involved in the investigation and enforcement of justice. The results of this study can be used to improve criminal legislation, in particular, to introduce amendments and additions to Chapter 4 of the Criminal Procedure Code concerning the definition of the very concept of "electronic (digital) evidence" and requirements for their relevance and admissibility.

Acknowledgements

None.

Conflict of Interest

None.

References

[1] About registered criminal offenses and the results of their pre-trial investigation. (2022). Retrieved from https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

[2] Abraha, H.H. (2021). Law enforcement access to electronic evidence across borders: Mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, 29(2), 118-153. doi: 10.1093/ijlit/eaab001.

[3] Cerbo, S. (2016). *Digital evidence changing the paradigm of human rights protection*. Oisterwijk: Wolf Legal Publishers.

[4] Chan, G., & Magotiaux, S. (2021). *Digital evidence*. In B.H. Greenspan, & V. Rondinelli (Eds.). Toronto: Emond Publishing.

[5] Depauw, S. (2018). Electronic evidence in criminal matters: How about E-Evidence instruments 2.0? *European Criminal Law Review (EuCLR),* 8(1), 62-82. doi: 10.5771/2193-5505-2018-1-62.

[6] Dublin Core metadata element set version 1.1: Reference description. (1999). Retrieved from https://old.library.kr.ua/dc/dcmi1_1u.html.

[7] Fil, O., & Khoynatska, L. (2022). Looting as a way of waging war by the Russian Federation against Ukraine and a motivational factor for Russian servicemen. *Ukrainian Historical Journal*, 4, 129-138. doi: 10.15407/uhj2022.04.129.

[8] Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross,* 102(913), 287-334. doi: 10.1017/S1816383120000387.

[9] Kancauskiene, J. (2019). Computer forensics and electronic evidence in criminal legal proceedings: Lithuania's experience. *Digital Evidence and Electronic Signature Law Review*, 16, 11-24.

[10] Khashashneh, T., Al-Billeh, T., & Abu Issa, H. (2022). The authority of the criminal judge to assess digital (electronic) evidence in Jordanian, Egyptian, and French legislation. *Journal of Southwest Jiaotong University*, 57(5), 631-640. doi: 10.35741/issn.0258-2724.57.5.51.

[11] Kostenko, M.V. (2019). Peculiarities of the innovative process in the field of criminology. In *Materials of the international "round table" conference* (pp. 72-75). Kharkiv: Pravo.

[12] Lasaka, M. (2023). Ius constituendum of electronic evidence arrangement in criminal procedure law. *Journal of Legality*, 16(2), 154-166.

[13] Latysh, K. (2022). Digital forensics during the war in Ukraine: Possibilities of using special knowledge in the field of information technologies. *Mykolas Romeris University Research Management System (CRIS),* 18, 18-21.

[14] Lewulis, P. (2021). Digital forensic standards and digital evidence in Polish criminal proceedings. An updated definition of digital evidence in forensic science. *International Journal of Electronic Security and Digital Forensics*, 13(4), article number 403. doi: 10.1504/IJESDF.2021.10034988.

[15] Mamedov, H. (2022). *Digital forensics. How did it help gather evidence of the Bucha crimes?* Retrieved from https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html.

[16] Marcello, D. (2015). Evidence gathering in the realm of the European investigation order: From national rules to global principles. *New Journal of European Criminal Law,* 6(2), 179-194. doi: 10.1177/203228441500600203.
[17] Murzo, Ye.O. (2023). Peculiarities of the appointment and conduct of certain types of forensic examinations in the investigation of looting. In *Criminal Justice: Current State and Development Prospects* (pp. 185-187). Kyiv: National Academy of Internal Affairs.
[18] Okpara, J., Uguru, U., Agom, C., & Mgbolu, A. (2023). Admissibility of electronic evidence in criminal trials in Nigeria and the challenges of new crimes. *AGORA International Journal of Juridical Sciences,* 1, 28-46.
[19] Predmestnikov, O., Nazarenko, P., & Pershina, K. (2023). Criminal liability for pillage in wartime conditions (Ukrainian realities). *Academic Visions*, 20, 1-9. doi: 10.5281/zenodo.8002682.
[20] Riekkinen, J. (2019). Electronic evidence in criminal procedure: On the effects of ICT and the development towards the network society on the life-cycle of evidence. *Digital Evidence and Electronic Signature Law Review*, 16, 6-10.
[21] Rojszczak, M. (2022). E-Evidence cooperation in criminal matters from an EU perspective. *Modern Law Review*, 85(4), 997-1028. doi: 10.1111/1468-2230.12749.
[22] Sabadin, A. (2021). *How to submit an electronic proof to be accepted?* Retrieved from https://yur-gazeta.com/publications/practice/sudova-praktika/yak-podati-elektronniy-dokaz-abi-yogo-priynyali.html.
[23] Shepitko, V., & Shepitko, M. (2021). Doctrine of criminalistics and forensic examination: Formation, current state and development in Ukraine. *Law of Ukraine*, 8, 12-27.
[24] Stefaniv, N. (2022). *Judicial practice of the Supreme Court of Ukraine regarding the admissibility of electronic evidence.* Retrieved from https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf.
[25] Tosza, S. (2020). All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order. *New Journal of European Criminal Law,* 11(2), 161-183. doi: 10.1177/2032284420919802
[26] Wang, B., & Liu, Y. (2019). Collection and judgment of electronic data evidence in criminal cases: From the perspective of investigation and evidence collection by public security organs. *Journal of Forensic Science and Medicine,* 5(4), 187-194. doi: 10.4103/jfsm.jfsm_26_19.
[27] Yanovska, O. (2022). *The procedure for collecting and recording e-evidence must necessarily involve computer technology specialists.* Retrieved from https://radako.com.ua/news/procedura-zboru-ta-fiksaciyi-e-dokaziv-obovyazkovo-maie-vklyuchati-fahivciv-kompyuternih.

Використання електронних доказів як засобу доказування під час розслідування мародерства

Євгенія Мурзо
Ад'юнкт
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0009-0000-4409-0560

Вікторія Гальченко
Ад'юнкт
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0009-0000-7164-2949

■ **Анотація.** Електронні докази стають одними з ключових складових розслідування кримінальних правопорушень. Використання цифрових доказів дає змогу розслідувати не лише кримінальні правопорушення проти власності, довкілля тощо, а й правопорушення, вчинені в період війни та окупації. З початку широкомасштабного вторгнення в Україну збільшилася кількість випадків мародерства, про які стає відомо з відкритих джерел інформації. Метою цієї роботи було дослідження проблемних питань використання цифрових доказів у процесі розслідування мародерства. Методологічним підґрунтям слугували загальнонаукові методи пізнання, а саме наукової абстракції, дедукції та індукції, екстраполяції та логічного узагальнення. У статті здійснено дослідження мародерства серед інших воєнних злочинів у контексті визначення поняття, складу злочину, допустимості цифрових доказів під час розслідування цього злочину. Обґрунтовано нагальність вирішення проблемних аспектів, пов'язаних із розслідуванням мародерства, передусім у контексті повномасштабної війни в Україні. Відмежовано мародерство від інших злочинів проти власності, які вчинено в умовах воєнного або надзвичайного стану. Розглянуто проблематику термінології та окреслено підходи до кваліфікації кримінальних правопорушень, вчинених в умовах воєнного стану, а також недоліки законотворчості. Запропоновано внести зміни до Кримінального процесуального кодексу України, визначивши вимоги до електронних доказів під час розслідування мародерства. Практичне значення роботи полягає в тому, що такі інструменти можна застосовувати для подальших досліджень питання використання цифрових доказів як засобу доказування під час розслідування мародерства, у межах розроблення та вдосконалення законодавства за цим напрямом

■ **Ключові слова:** цифрова криміналістика; джерела інформації; цифровізація; кримінальне правопорушення; воєнні злочини; воєнний стан