UDC 343.132:343.137.5:343.982
DOI: 10.56215/naia-herald/2.2023.52

# Extraction of information from a cellular phone (mobile communication device) during investigative (search) actions

**Mykola Kobets***
PhD in Law, Associate Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-2233-0946

■ **Abstract.** The relevance of the study is substantiated by the need to develop a system for procedural registration of information (statements) withdrawn from a mobile phone using hardware and software complexes, the content of which proves the involvement of a person in the commission of a criminal offence, since such a documentation mechanism has not been developed in practice. The purpose of the study was to highlight theoretical and applied approaches to the legal support of investigators' actions to extract information from a mobile phone found at the incident scene. In accordance with the set goal and specifics of the subject of research, a set of the following methods was applied: formal logical, system and structural, hermeneutical, modelling, and generalisation. The study considers the actions of the investigator during the pre-trial investigation of criminal offences, when a cellular phone (mobile communication device) was found at the incident scene, which makes it necessary to use special knowledge. The profile and qualification of a specialist who needs to be involved in the inspection of a mobile phone are determined depending on the purpose and objectives of the investigative (search) action, established primary data on the nature of a criminal offense. A procedure for obtaining information (computer data) from a cellular phone (mobile communication device) is proposed, which provides for the creation of an "image"/electronic report of available information, which is recorded on a digital medium in the form of a file, fixed with an electronic label as a checksum. The practical value of the study lies in the procedural solution of the issue of extracting information (statements) from mobile phones, which is important during pre-trial investigation and documentation of digital information (computer data)

■ **Keywords:** computer data; protocol; mobile terminal; hardware and software complex; pre-trial investigation; specialist; special knowledge

■ **Suggested Citation:**
Kobets, M. (2023). Extraction of information from a cellular phone (mobile communication device) during investigative (search) actions. *Scientific Journal of the National Academy of Internal Affairs,* 28(2), 52-60. doi: 10.56215/naia-herald/2.2023.52.

■ *Corresponding author

■ Received: 16.03.2023; Revised: 02.06.2023; Accepted: 26.06.2023

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

## Introduction

With the rapid development of scientific and technological progress, humanity is increasingly using modern innovative technologies both in its professional activities and in everyday life. However, despite the technical capabilities of modern information systems and electronic communication networks, information technologies are vulnerable to fraudsters and other criminal elements. Such illegal actions are protected by law. This is especially true for the storage, use and dissemination of confidential information about a person without their consent. Law enforcement officers in certain situations, if it concerns the protection of national security interests, economic well-being and human rights are allowed to exercise these temporary restrictions, as defined by law, but only by a court decision (Article 32 of the Constitution of Ukraine[1]). Therefore, law enforcement officers use the entire arsenal of technological progress in their activities to detect, stop and investigate criminal offences.

In this regard, in order to clarify the circumstances of the commission of a criminal offence and establish the truth in criminal proceedings, there is an urgent need for data obtained from electronic information devices and systems. This is due to the fact that criminals have become more likely to use modern information and computer technologies in their illegal activities. To solve this problem, effective detection, suppression and investigation of relevant criminal offences and considering the realities of today, the legislator introduced in the CPC of Ukraine[2] such investigative (search) actions as the extraction of information from electronic information systems and the examination of mobile terminals (mobile communication devices) at the accident scene.

Theoretical and applied approaches to the use of electronic (digital) evidence in criminal proceedings were studied by I.V. Pyrih (2019), I. Riadi *et al.* (2023). They suggest using various forensic methods, tools, and software products to process and analyse the data obtained. A. Leonov (2020), S. Satpathy & S. Mohanty (2020) highlight issues of so-called digital forensics. In this context, the researchers suggest using data analysis methods, algorithms, and synthesis techniques to effectively investigate crimes committed using information technologies. A. Fukami *et al.* (2021) introduce a new forensic model for mobile device research. In their opinion, this is due to the convenience of using digital evidence, considering the elements of vulnerabilities and features of this type of evidence.

A. Sengupta *et al.* (2023), H. Tara & A. Mishra (2021) explore the problems of extracting internet data from mobile phones and other electronic devices, as well as digital forensic tools for this. To solve these problems, reasonable methods of data extraction are proposed, which work independently of the hardware and software specifications of the mobile terminal. B.M. Manjre *et al.* (2023) examine the integrity of digital evidence obtained during the extraction and decoding of mobile data from mobile phones, etc. The authors suggest using various information technologies to ensure security against possible changes and distortions of information during its extraction from mobile terminals and features of storing digital evidence during forensic examinations.

The purpose of the study was to help employees of the pre-trial investigation bodies to obtain the necessary information from mobile terminals (cellular phones) found at the scene during the pre-trial investigation of criminal offences, using modern scientific and technical means, and procedural registration of the seized information, which can be further evidence in criminal proceedings.

## Materials and Methods

In the course of the study of the problem of extracting (copying) information by investigators from the mobile communication device, methodological tools were used. The combination of both general scientific and special methods of scientific cognition was used to achieve the outlined goal of research. The fundamental basis of the methodology in this paper is the dialectical approach, which allows substantiating objectivity in assessing reality. In this context, the method of dialectics is applied in order to expand the terminology by analysing the problems of extracting (copying) and documenting evidence (forensically significant information) at the scene, using modern scientific and technical technologies for obtaining data and areas for solving relevant issues.

During the research, a system of methods of scientific cognition was used. The formal logical method (abstraction, logic, induction, deduction, synthesis) was used to clarify the content of the issues under study. That is, to build a procedure for identifying information from mobile terminals, starting from the moment of receiving information about the commission of a criminal offence and ending with the procedural registration of the seized information at the scene of the incident. Using the hermeneutical method, the concepts of "inspection of objects", "data", and "computer data" used in legislative acts and of legal and practical significance in criminal proceedings were studied. Therefore, these concepts were generalised to reconcile further contradictions and compare the relationship between the concepts of "computer information" and "digital information".

[1]Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
[2]Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

The analytical method was used in the process of research of academic literature, the analysis of which provided an opportunity to compare opinions and ways to solve relevant problematic issues, and as a result, to provide a solution to the extraction of information from mobile terminals. The system and structural method was used for a comprehensive scientific analysis of ways to document digital information at the accident scene. Using the modelling, the sequence of actions of employees of the pre-trial investigation body during the investigation of criminal offences was developed. The generalisation was used to formulate conclusions.

In preparing the paper, the author has considered foreign and Ukrainian literature on the problematic issues of such scholars as A. Leonov (2020), H. Tara & A. Mishra (2021), J. Williams *et al.* (2021). The study used the provisions of legislative acts – the CPC – as a material basis[1], which provides for the procedure for actions of pre-trial and judicial investigation bodies in the investigation of a criminal offence within the framework of criminal proceedings and the laws of Ukraine "On Electronic Communications"[2], "On Electronic Trust Services"[3].

## Results

Investigative (search) actions at the accident scene are carried out in order to identify, evaluate, and examine evidentiary information that may be relevant for criminal proceedings (Nassif, 2019; Riadi *et al.,* 2023). The investigator applies the existing arsenal of scientific and technical developments, since they are responsible for the course of the pre-trial investigation (Wang *et al.,* 2018; Karthikeyan *et al.,* 2023). In case of detection and seizure of mobile communication equipment at the place of commission of a criminal offence, the investigator initiates the use of a hardware and software complex that is used within the framework of:

- conducting such an investigative (search) action as inspection of the area, premises, things, documents and computer data (Article 237 "Inspection" of the Criminal Procedure Code (CPC) of Ukraine[4]) – for inspection of a mobile phone and/or SIM card;

- criminal proceedings during such an investigative (search) action as a search of a person's home or other possession, a search of a person (Article 236 "Execution of a Decision on a Permit to Search a Person's Home or Other Possession" of the CPC of Ukraine[5]) – for access to computer systems or parts thereof, mobile phones and/or SIM cards.

If a mobile phone was found at the place of commission of a criminal offence or a person suspected of committing a criminal offence was or was detained at the scene and a mobile communication device was found in their possession, the investigator as part of the investigation team initiates such an investigative (search) action as an inspection of the area, premises, things, documents, and computer data in accordance with Article 237 of the CPC of Ukraine "Inspection"[6] in order to identify and record information about the circumstances of the commission of a criminal offence. At the same time, they carry out not only its external inspection as an object, but also internal – the content of information contained in this device, as an inspection of computer data, since information about illegal activities of a person can be stored in a mobile phone (Perumal *et al.,* 2017). Given the technical specificity of this device due to its operation, and in order to obtain assistance on issues requiring special knowledge for such actions, the investigator (prosecutor) may invite a specialist to participate in this review (Pyrih, 2019).

Usually, the investigator engages an employee of the operational and technical unit as a specialist in these actions in accordance with Part 3 of Article 237 and Article 71 of the CPC of Ukraine[7]. The specialist in accordance with paragraph 1 of Part 5 of Article 71 of the CPC of Ukraine[8] must "arrive on call to the investigator, inquirer, prosecutor, court and have the necessary technical equipment and devices"[9]. Therefore, the investigator informs their supervisor from the scene of the incident about the need to involve a specialist with a hardware and software complex (Wang *et al.,* 2018; Kayabaş & Tuna, 2023). The investigator records the participation of a specialist in the protocol of examination of the subject.

For an in-depth understanding of the relevant investigative (search) action related to the technical feature of the operation of a mobile communication device found at the scene, the concept of "inspection of objects and computer data" should be considered, which may be relevant in criminal proceedings. In general, the inspection of things provides for actions related to the external inspection of the object

[1]Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2]Law of Ukraine No. 1089-IX "On Electronic Communications". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1089-20#Text.
[3]Law of Ukraine No. 2155-VIII "On Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19/ed20220101#top.
[4]Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[5]Ibidem, 2012.
[6]Ibidem, 2012.
[7]Ibidem, 2012.
[8]Ibidem, 2012.
[9]Ibidem, 2012.

(substances, etc.) with an indication of the features of the signs of this object, which allows distinguishing it from identical ones. As a rule, such actions at the scene of an accident as part of the investigation team are carried out by a forensic inspector[1]. The legislative acts of Ukraine regulating the activities of law enforcement agencies do not use such concepts as "computer information", "digital information", etc., i.e., information that is extracted from electronic (information) communication devices.

However, the CPC of Ukraine provides for the use of the concept of "computer data" (Articles 99, 237)[2]. In this context, the Convention on cybercrime, Article 1, interprets this concept as information that is suitable for processing (performing certain functions) in a computer system[3]. That is, computer data contains both information and a programme for performing certain actions of the computer system. The interpretation of this concept is difficult to compare with electronic communication devices and systems, since they do not belong to the concept of a computer. At the same time, data is information in a form suitable for automated processing by computer technology, technical and software tools (paragraph 20 of Part 1 of Article 2)[4]. An electronic data – any information in electronic form (paragraph 13 of Part 1 of Article 1)[5]. Therefore, data is information presented in electronic form. In the field of forensics, scientists correlate the concepts of "electronic data" and "computer data" with the concepts of "computer information" and "digital information" (Teplytskyi, 2020; Hutsaliuk & Antoniuk, 2021). In general, computer data is information that is processed in devices, systems, etc.

A specialist at the accident scene in the presence of witnesses uses a hardware and software complex such as Cellebrite UFED or its analogue to inspect the computer data of a mobile phone detected and seized by an investigator, that is, information, and creates an "image"/electronic report of available information (Tara & Mishra, 2021). The person performing these procedural actions certifies the recorded information on the digital disk with an electronic signature. In accordance with the legislation of Ukraine in the fields of electronic trust services and electronic identification, in particular, the decision of the Supreme Court of Ukraine of the panel of judges of the Commercial Court of Cassation in case No. 922/51/20 of January 29, 2021, an electronic signature is equated to a handwritten signature[6], in accordance with paragraph 12 of Article 1 of the Law of Ukraine "On Electronic Trust Services"[7].

A specialist writes the created "image"/electronic report to a digital medium, such as a digital disc such as CD-R, DVD-R in the form of a file, and attaches an electronic tag in the form of a checksum using the mathematical (cryptographic) algorithm SHA-1 (or SHA-2, SHA-3, MD5, CRC32) (Kobets, 2023). According to the CPC, the inspection of computer data is carried out by an investigator (prosecutor), reflecting it in the inspection protocol, in accordance with Part 2 of Article 237 of the CPC of Ukraine[8]. The investigator draws up a report in accordance with Article 104 of the CPC of Ukraine[9]. A mobile phone, a tangible medium of information marked by a specialist with a mathematical hashing algorithm SHA-1 (or SHA-2, SHA-3, MD5, CRC32) with information obtained during the inspection of information from mobile communication devices and/or SIM cards (Article 105 of the CPC of Ukraine)[10]. The protocol is signed by all participants who participated in the procedural action in accordance with Part 5 of Article 104 of the CPC of Ukraine[11].

Considering the protocol registration of the evidence base, it is worth noting that Article 84 of the CPC of Ukraine states that the sources of evidence are testimony, material evidence, documents, and expert conclusions. According to paragraph 1 of Part 2 of Article 99 of the CPC of Ukraine, documents may include materials of photography, sound recordings,

[1]Order of the Ministry of Internal Affairs of Ukraine No. 575 "On Instructions on the Organisation of the Interaction of Pretrial Investigation Bodies with Other Bodies and Units of the National Police of Ukraine in the Prevention of Criminal Offences, Their Detection and Investigation". (2017, July). Retrieved from https://zakon.rada.gov.ua/laws/show/z0937-17#Text.
[2]Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[3]Law of Ukraine No. 2824-IV "On Convention on Cybercrime". (2005, September). Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text.
[4]Law of Ukraine No. 1089-IX "On Electronic Communications". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1089-20#Text.
[5]Law of Ukraine No. 2155-VIII "On Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19/ed20220101#top.
[6]Resolution of the Commercial Court of Cassation of the Supreme Court of Ukraine case No. 922/51/20. (2021, January). Retrieved from https://verdictum.ligazakon.net/document/94517830.
[7]Law of Ukraine No. 2155-VIII "On Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19/ed20220101#top.
[8]Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[9]Ibidem, 2012.
[10]Ibidem, 2012.
[11]Ibidem, 2012.

video recordings, and other information carriers (including computer data)[1]. In practice, sometimes there are legal situations when the defender challenges the actions of the investigator regarding the inadmissibility of evidence, that is, the illegality of the inspection of a mobile phone without the approval of the investigating judge, considering that during investigative (search) actions illegal (without the decision of the investigating judge) access to information from electronic Information systems was carried out, which is issued as a protocol for the inspection of the object – phone (Leonov, 2020). However, this situation is explained by the decision of the Supreme Court of Ukraine of the panel of judges of the Criminal Court of Cassation in case No. 727/6578/17 of April 15, 2020. According to its decision, a mobile phone does not belong to the concept of "electronic information systems or parts thereof", so it is legitimate to carry out an internal inspection (its informational content) of this phone by investigators without a court decision[2].

Commenting on the decision of the Supreme Court, it is worth considering the concept of a mobile phone, namely, as a means of mobile communication. In accordance with the legislation of Ukraine in the field of electronic communications[3], a cellular phone as a mobile terminal is the final element of an electronic communication network, in particular, mobile communication. Therefore, a mobile phone does not apply to electronic information systems. If a person detained on suspicion of committing a criminal offence voluntarily provided investigators with access to information (computer data) of their mobile phone, then in this case, the use of a hardware and software complex is not mandatory, since one of the main functions of this complex is to overcome the system of logical protection of mobile terminals. However, in this situation, it should be noted in the report on the inspection of the object that they were given this opportunity voluntarily.

Within the framework of criminal proceedings, when conducting such an investigative (search) action as a search of a person's home or other possession, a search of a person (Article 236 of the CPC of Ukraine "Execution of a Decision on Permission to Search a Person's Home or Other Possession"[4]) to access computer systems or parts thereof, mobile phones (means of mobile communication) and/or SIM cards, also involve a specialist to inspect the mobile terminal (mobile phone) and SIM card directly at the place of the search with its subsequent inspection. To carry out the relevant procedural action, the investigator involves a specialist in accordance with Part 1 of Article 236 and Article 71 of the Criminal Procedure Code of Ukraine[5]. In such a case, the investigator issues an appropriate decision in accordance with Part 3 of Article 110 of the CPC of Ukraine[6]. The CPC provides that during a search, an investigator has the right to overcome logical protection systems, record computer data in accordance with Part 6 of Article 236 of the CPC of Ukraine[7]. In case of detection of a mobile phone and/or SIM card during a search of the premises, the procedure for using a hardware and software complex such as Cellebrite UFED or its analogue (Tara & Mishra, 2021), extracting information from the mobile terminal and further documenting it is similar to the procedural action for inspection. If necessary, the investigator sends a digital carrier with the created "image"/electronic report of the seized mobile phone to a specialist to analyse the information extracted from the created "image".

Thus, the information provided can expand the procedural activities of employees of the pre-trial investigation body regarding the legally correct solution of practical issues, if a mobile phone is found at the place of committing a criminal offence, the information of which may have evidentiary value in criminal proceedings. The described procedure provides for proper protection of the rights of the person under study and compliance with legal requirements in the context of conducting a search, attracting a specialist and preserving the integrity and objectivity of evidence in criminal proceedings.

## Discussion

In their publications, the researchers carried out a comparative study of the means of extracting (copying) forensic information (computer data) from mobile terminals, in the field of electronic communication and information systems, which may be of practical importance. H. Bowling *et al.* (2023) conducted a detailed forensic analysis of the Microsoft Teams programme on Windows 10, iOS, and Android operating systems for investigators (detectives) to recover forensic data from the Teams programme. The software used was checkra1n 0.12.2, as well as

[1]Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[2]Resolution of the Second Judicial Chamber of the Criminal Court of Cassation, Supreme Court case No. 727/6578/17. (2020, April). Retrieved from https://zakononline.com.ua/court-decisions/show/88749345
[3]Law of Ukraine No. 1089-IX "On Electronic Communications". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1089-20#Text.
[4]Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[5]Ibidem, 2012.
[6]Ibidem, 2012.
[7]Ibidem, 2012.

TWRP, a tool that allows installing firmware from unidentified developers. To extract information from mobile phones with the iOS and Android operating systems, the Cellebrite UFED 4pc hardware and software package version 7.42.0.82 and the magnet AXIOM Examine analytics tool were used. During this analysis, it turned out that when the memory capacity of a mobile phone is larger than the capabilities of a hardware and software complex, simultaneous physical extraction of information is almost impossible. Therefore, the researchers suggest using other methods for extracting and analysing data from mobile communications. However, their proposed method is difficult to use in practice.

By analysing and comparing the most common mobile forensic tools used to extract information from electronic information devices and systems, such as FTK Imager, Encase, Paladin Suite, Cellebrite, Oxygen forensic tool, and Tableau hardware, the researchers concluded that the FTK Imager image processing programme is simpler and faster to use than EnCase. It was found that the Cellebrite UFED hardware and software suite is better than the Oxygen forensic tool in terms of ease of maintenance, although it is almost identical in terms of technical capabilities (Tara & Mishra, 2021). H. Kayabaş & G. Tuna (2023) emphasised the importance and necessity of using Cellebrite hardware and software complexes with UFED 4pc software by investigators or/or specialists during pre-trial investigations. The researchers' proposal is related to the fact that the Cellebrite UFED hardware and software package uses software to extract (copy) important data from a mobile phone, which can later help law enforcement officers establish the facts of a person's involvement in the commission of a criminal offence. For example: phone books, photos, videos, text messages, call logs, ESN and IMEI data, and then collects the data in a report for research and evidence collection. The issue of the effectiveness of using tools by specialists to extract digital information from mobile communication tools was also considered by S. Saleem *et al*. (2016). Their research was based on the use of a mathematical method for evaluating the Cellebrite UFED and MSAB XRY hardware and software complexes. The results of the comparison showed that XRY in most cases met the performance and compliance requirements better than UFED.

P. Wang *et al.* (2018) investigating the effectiveness of using forensic methods for extracting digital information from mobile devices, proposed to use different hardware and software complexes simultaneously. Their opinion is based on the fact that each complex has its own advantages and disadvantages. Combining two complexes with different capabilities can provide maximum results, that is, remove information from devices as much as possible. This conclusion was made as a result of empirical data demonstrating the advantages of integrating the strengths of two different hardware and software complexes, such as Cellebrite UFED 4pc and Oxygen Forensics. Therefore, they tend to take an integrated approach to the capabilities of mobile forensic tools through their combined use.

Studying the practical application of hardware and software complexes for extracting information from devices, the researchers propose to expand the possibilities of using Cellebrite UFED and MSAB XRY hardware and software complexes for obtaining data from fitness bracelets (Kobets, 2023). This is due to the fact that fitness bracelets can store such data as a person's location (GPS), speed, and pulse at a certain time, i.e., their psychological state. If a suspect who was caught at the scene of a criminal offence, or was at a distance from the scene of the accident, a smart watch or fitness bracelet can be found using a hardware and software complex, which may later have evidentiary value in criminal proceedings (Williams *et al.,* 2021). Getting information from mobile phones such as iPhones with the iOS operating system has certain difficulties, especially when it comes to social media applications. To solve this problem, M.S. Al-Faaruuq & D.F. Priambodo (2022) suggest using tools such as Cellebrite UFED 4pc, Oxygen Forensic Detective, FTK Imager, and Autopsy. The result of using such tools has high indicators.

When using software products of social networks, information fingerprints remain in mobile phones, which in certain situations may be of interest to law enforcement officers, according to Y. Keim *et al.* (2022). To obtain the necessary data, the researchers carried out a forensic analysis. At the same time, Magnet AXIOM Process and Cellebrite UFED 4pc tools were used to obtain the necessary information from the mobile phone for data collection, as well as Magnet AXIOM Examine and DB Browser for SQLite for analysis and reading. Investigating the problem of extracting mobile forensic evidence, S. Perumal *et al.* (2017), G. Dorai *et al.* (2018) conducted comparative studies of open-source software to extract deleted data, and extract other important information from a mobile phone with the Android operating system. Considering the issue of facilitating the work of individuals who collect, store and use forensic (digital) evidence, the researchers propose to create such a forensic tool as the Forensic Evidence Acquisition and Analysis System (FEAAS). This system consolidates the evidence into a readable report that identifies user events (e.g., logging in or out of a device) and what triggered the event (or the use of an IOS mobile phone application).

In the process of studying social networks that are used to spread false information, extremist ideologies, etc., there is a problem of extracting and recording such illegal distribution. The result of this

study showed that some apps store unencrypted user information on devices, such as usernames, phone numbers, email addresses, posts and comments, and private chat messages. In addition, the authors discovered some security vulnerabilities that allow users to upload data that was supposed to be private (for example, sent private images) without authentication or authorisation by other users. To solve this problem, H. Johnson *et al.* (2022) suggest using the Alternative Social Networking Applications Analysis Tool (ASNAAT), which automatically responds to criminally relevant data from alternative social media technologies when presented with a forensic image of a mobile device.

Studying the issues of extracting and analysing data from cell phones, I. Idris *et al.* (2016) suggest obtaining the necessary information for investigation from SIM and USIM cards using appropriate software tools. The above analysis of the use of forensic methods and tools for the extraction and analysis of forensic significant information from mobile communication tools provides investigators and specialists with the opportunity to navigate and make a choice, that is, which tools are best used to obtain information from modern devices and systems.

## Conclusions

The study has developed a method for obtaining (extracting) digital (electronic) information from mobile phones using forensic software tools. This process is very important for law enforcement agencies, as it allows obtaining evidence from mobile phones during the investigation of criminal proceedings. The methodology includes the use of technical capabilities of special equipment and software for receiving and processing information from mobile phones. The law also sets out the procedure for processing this information at the scene of a criminal offence for further use as evidence in criminal proceedings.

Procedural actions are given during which the investigator can initiate the use of a hardware and software complex such as Cellebrite UFED or its analogues to extract information from a mobile phone and/or SIM cards found at the incident scene during such investigative (search) actions as inspection and search. A procedural sequence of actions of investigators during the pre-trial investigation of criminal offences related to obtaining the necessary information (computer data) from a mobile phone has been developed, which provides for the creation of an "image"/electronic report of available information, which is recorded on a material digital medium in the form of a file, fixed with a mathematical electronic label in the form of a checksum.

Considering legal discussions about the inadmissibility of evidence when receiving information from mobile terminals seized from detained persons suspected of committing a criminal offence, investigators substantiated the legality of using hardware and software complexes such as Cellebrite UFED or its analogues to extract information from mobile phones. The reasoning is based on a comment on the decision of the Supreme Court of Ukraine of the panel of judges of the Criminal Court of Cassation in case No. 727/6578/17 of April 15, 2020. For an in-depth understanding of such an investigative (search) action as the inspection of objects and computer data, in accordance with Article 236 of the CPC of Ukraine, and considering the technical features of the operation of a mobile phone found at the scene, the concept of "inspection of objects", "computer data", "data", which may be relevant in criminal proceedings, is considered.

The scientific originality of the study lies in the fact that it offers a sequence of actions of the investigator in case of detection of a mobile phone at the scene and a procedural procedure for extracting (copying) information (computer data) from this device, using the technical capabilities of the hardware and software complex. The provided scientific and methodological recommendations in the process of presenting the main material can form the methodological basis for the effective detection and investigation of criminal offences of this nature. An important factor is the cooperation of practitioners and the scientific community on new software complexes, the development of innovative methodologies, the conduct of individual forensic studies, and the launch of the latest technologies.

## Acknowledgements

None.

## Conflict of Interest

None.

## References

[1] Al-Faaruuq, M.S., & Priambodo, D.F. (2022). IOS digital evidence comparison of instant messaging apps. In *International conference of science and information technology in smart administration (ICSINTESA)* (pp. 83-88). New York: Institute for Electrical and Electronics Engineers. doi: 10.1109/ICSINTESA56431.2022.10041620.

[2] Bowling, H., Seigfried-Spellar, K., Karabiyik, U., & Rogers, M. (2023). We are meeting on Microsoft Teams: Forensic analysis in Windows, Android, and iOS operating systems. *Journal of Forensic Sciences*, 68(2), 434-460. doi: 10.1111/1556-4029.15208.

[3] Dorai, G., Houshmand, S., & Baggili, I. (2018). I know what you did last summer: Your smart home internet of things and your iPhone forensically ratting you out. In *ARES 2018: Proceedings of the 13th international conference on availability, reliability and security* (pp. 1-10). New York: Association for Computing Machinery. doi: 10.1145/3230833.3232814.

[4] Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation,* 38, article number 301169. doi: 10.1016/j.fsidi.2021.301169.

[5] Hutsaliuk, M.V., & Antoniuk, P.Ye. (2021). The essence of digital information a source of evidence in criminal proceedings. *Forensic Herald*, 33(1), 37-49. doi: 10.37025/1992-4437/2020-33-1-37.

[6] Idris, I., Alhassan, J.K., Waziri, V.O., & Majigi, M.U. (2016). SIM cards forensic capability and evaluation of extraction tools. In *International conference on information and communication technology and its applications (ICTA 2016)* (pp. 75-81). Minna: Federal University of Technology.

[7] Johnson, H., Volk, K., Serafin, R., Grajeda, C., & Baggili, I. (2022). Alt-tech social forensics: Forensic analysis of alternative social networking applications. *Forensic Science International: Digital Investigation*, 42, article number 301406. doi: 10.1016/j.fsidi.2022.301406.

[8] Karthikeyan, P., Pande, H.M., & Sarveshwaran, V. (Eds.). (2023). *Artificial intelligence and blockchain in digital forensics*. New York: River Publishers. doi: 10.1201/9781003374671.

[9] Kayabaş, H., & Tuna, G. (2023). Cyber wars and cyber threats against mobile devices: Analysis of mobile devices. In *Handbook of research on war policies, strategies, and cyber wars* (pp. 85-107). doi: 10.4018/978-1-6684-6741-1.ch005.

[10] Keim, Y., Hutchinson, S., Shrivastava, A., & Karabiyik, U. (2022). Forensic analysis of TikTok alternatives on android and iOS devices: Byte, dubsmash, and triller. *Electronics*, 11(18), article number 2972. doi: 10.3390/electronics11182972.

[11] Kobets, M.V. (2023). "Cellebrite UFED" hardware and software complex as a means of obtaining information from mobile terminals. In *Current issues and prospects for the use of investigative tools in solving crimes under martial law: Material interdepartmental science and practice conferences* (pp. 70-73). Kyiv: National Academy of Internal Affairs.

[12] Leonov, A. (2020). *Intrusion into privacy*. Retrieved from https://zib.com.ua/ua/142223.html.

[13] Manjre, B.M., Goyal, K.K., & Shivani. (2023). A novel and custom blockchain approach for the integrity assurance of the digital evidences extracted during the extraction and decoding of mobile artifacts from the mobile forensic tools. *Advances in Material Science and Manufacturing Engineering*, 2753(1), article number 030006. doi: 10.1063/5.0127910.

[14] Nassif, L.N. (2019). Conspiracy communication reconstitution from distributed instant messages timeline. In *Institute for Electrical and Electronics Engineers (IEEE) wireless communications and networking conference workshop* (pp. 1-6). New York: Institute for Electrical and Electronics Engineers. doi: 10.1109/WCNCW.2019.8902574.

[15] Perumal, S., Navarathnam, S., De Vosse, C., Samsuddin, S.B., & Samy, G.N. (2017). Comparative studies on mobile forensic evidence extraction open source software for android phone. *Advanced Science Letters*, 23(5), 4483-4486. doi: 10.1166/asl.2017.8922.

[16] Pyrih, I.V. (2019). Involvement of specialists in investigative activities in the investigation of criminal offenses. In *Realities and prospects for the development of the rule-of-law state in Ukraine and worldwide* (pp. 93-122). Lviv: Liha-Pres. doi: 10.36059/978-966-397-207-7/93-122.

[17] Riadi, I., Yudhana, A., & Inngam Fanani, G.P. (2023). Mobile forensic tools for digital crime investigation: Comparison and evaluation. *International Journal of Safety and Security Engineering,* 13(1), 11-19. doi: 10.18280/ijsse.130102.

[18] Saleem, S., Popov, O., & Baggili, I. (2016). A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis. *Digital Investigation,* 16, S55-S64. doi: 10.1016/j.diin.2016.01.008.

[19] Satpathy, S., & Mohanty, S. (Eds.). (2020). *Big Data Analytics and computing for digital forensic investigations*. Boca Raton: Chemical Rubber Company Press. doi: 10.1201/9781003024743.

[20] Sengupta, A., Singh, A., & Vinjit, B.M. (2023). A platform independent and forensically sound method to extract WhatsApp data from mobile phones. *International Journal of Electronic Security and Digital Forensics*, 15(3), 259-280. doi: 10.1504/IJESDF.2023.130657.

[21] Tara, H., & Mishra, A. (2021). A comparative study of digital forensic tools for data extraction from electronic devices. *Journal of Punjab Academy of Forensic Medicine and Toxicology,* 21(1), 97-104. doi: 10.5958/0974-083X.2021.00016.9.

[22] Teplytskyi, B.B. (2020). Application of criminal tools during a search during investigation of crimes in the field of use of computers, systems and computer networks and telecommunications networks. *Legal Science,* 5(107), 151-157. doi: 10.32844/2222-5374-2020-107-5-2.19.
[23] Wang, P., Rosenberg, M., & D'Cruze, H. (2018). Integration of mobile forensic tool capabilities. In S. Latifi (Ed.), *Information technology – New generations. Advances in intelligent systems and computing* (pp. 81-87). Cham: Springer. doi: 10.1007/978-3-319-77028-4_13.
[24] Williams, J., MacDermott, A., Stamp, K., & Iqbal, F. (2021). Forensic analysis of Fitbit versa: Android vs iOS. In *2021 Institute for Electrical and Electronics Engineers (IEEE) symposium on security and privacy workshops* (pp. 318-326). San Francisco: Institute for Electrical and Electronics Engineers. doi: 10.1109/SPW53761.2021.00052.

# Вилучення інформації зі стільникового радіотелефону (засобу мобільного зв'язку) під час слідчих (розшукових) дій

**Микола Кобець**
Кандидат юридичних наук, доцент
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-2233-0946

■ **Анотація.** Актуальність статті обґрунтована необхідністю розроблення порядку процесуального оформлення інформації (відомостей), вилученої зі стільникового радіотелефону за допомогою апаратно-програмних комплексів, зміст якої доводить причетність особи до вчинення кримінального правопорушення, оскільки на практиці такий механізм документування не відпрацьовано. Мета статті полягала у висвітленні теоретико-прикладних підходів до правового забезпечення дій слідчих з вилучення відомостей зі стільникових радіотелефонів, виявлених на місці події. Відповідно до поставленої мети та специфіки предмета дослідження застосовано комплекс таких методів: формально-логічний, системно-структурний, герменевтичний, моделювання, узагальнення. Розглянуто дії слідчого під час досудового розслідування кримінальних правопорушень, коли на місці події виявлено стільниковий радіотелефон (засіб мобільного зв'язку), що зумовлює необхідність використання спеціальних знань. Профіль і кваліфікація фахівця, якого потрібно залучити до огляду стільникового радіотелефону (засобу мобільного зв'язку), визначають залежно від мети й завдань слідчої (розшукової) дії, встановлених первинних даних про характер кримінального правопорушення. Запропоновано процесуальний порядок отримання відомостей (комп'ютерних даних) зі стільникового радіотелефону (засобу мобільного зв'язку), що передбачає створення «образу»/електронного звіту наявної інформації, який записують на цифровий носій у вигляді файлу, закріплюють електронною міткою як контрольну суму. Практична цінність публікації полягає в процесуальному вирішенні питання вилучення відомостей (інформації) зі стільникових радіотелефонів, що важливо під час досудового розслідування та документування цифрової інформації (комп'ютерних даних)

■ **Ключові слова:** комп'ютерні дані; протокол; мобільний термінал; апаратно-програмний комплекс; досудове розслідування; спеціаліст; спеціальні знання