Identification of Person Suspected of Committing a Cybercrime Using Wi-Fi Technologies

Yuriy Nizovtsev * [a], Oleg Parfylo ** [b], Oleh Plakhotnik * [c]**

* PhD in Law, Ukrainian Research Institute of Special Equipment and Forensic Science of the Security Service of Ukraine, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-7641-6403, e-mail: nizovtsev.yurii@gmail.com
** PhD in Law, Ukrainian Research Institute of Special Equipment and Forensic Science of the Security Service of Ukraine, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-8787-7478, e-mail: parfylo.oleg@gmail.com
*** PhD in Law, Docent, Taros Shevchenko National University of Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-2787-6956, e-mail: knukyiv1@gmail.com

[a] Writing – original draft, Methodology, Formal analysis.
[b] Writing – original draft, Project administration, Methodology, Supervision.
[c] Writing – original draft, Methodology, Formal analysis, Resources.

DOI: 10.32353/khrife.4.2023.03 UDC 343.98:004.7
Submitted: 20.11.2023 / Reviewed: 22.11.2023 / Approved for Print: 18.12.2023 / Avialable online: 29.12.2023

This article purpose is to investigate the issue of using Wi-Fi routers and information they contain during the investigation of cybercrimes committed using Wi-Fi technology as a method effective for identifying suspect person or group of persons and subsequently determining their location. For achieving this goal, general scientific and special scientific research methods were applied. Various methodical recommendations on the use of Wi-Fi routers for mobile device installation by means of forensic research have been developed. It is emphasized that in case of committing cybercrime using a Wi-Fi router, a professional and forensic expert can use technical information from the Wi-Fi router to identify the suspect's mobile device by MAC address. Problematic issues of identifying signs of hiding digital traces during cybercrime commission a are considered. The procedure for obtaining access to Wi-Fi routers for the purpose of identifying suspect during inspection, search, seizure and investigation of

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

cybercrimes is outlined. Data from Wi-Fi routers has been proven to not only help identify criminal suspects in cybercrime investigations: this method can be universal for identifying criminal suspects with incomplete data. The "electronic data" term was analyzed, special role of a specialist in the review of electronic data was noted, and it was proposed to change the current Criminal Procedural Code of Ukraine in terms of specialist participation in electronic data review on behalf of investigator, prosecutor, and investigator during a pre-trial investigation of criminal cases. misdemeanors The provisions and conclusions of the author's research will be useful in investigative, investigative and forensic activities.

Keywords: *cybercrimes; routers; Wi-Fi technologies; electronic communications; electronic evidence; digital traces; investigations; forensic science; guidelines.*

Research Problem Formulation

The use of Wi-Fi routers and information they contain in cybercrime investigations can be an extremely effective method for the prosecution to locate a suspect and use technical information from such routers as digital evidence preserving digital cybercrime traces [1]. Wi-Fi routers are devices designed for wireless connection of mobile subscriber terminals with Internet and other network resources. Functionally, they route (direct in a certain direction) packets of information between wireless devices and the Internet. While communication, as user information (traffic of remote control commands, content of a website page, downloading of a certain file, transmission of a video stream, etc.) as service data necessary for operation of the network are transferred. Service data includes, among other things, information about a mobile device, while user information characterizes network activity and can contain cyberattack digital traces or other illegal activity. In addition, Wi-Fi router can contain certain information about service data and network activity, so-called logs. Moreover, after a suspect commits a cybercrime using a Wi-Fi router, specialist and forensic expert can use technical information from Wi-Fi router to identify the suspect's mobile device by MAC address. This information can be used by the prosecution to de-anonymize and find out the location of suspected person or group of persons and the real place of their access to the network based on such factual data. When applying this method, it is necessary to follow appropriate procedural procedures for obtaining information from the Wi-Fi router and its proper preservation for the purpose of further use of such information by the prosecution as evidence in criminal proceedings.

1 Омельян О. С. Поняття та ознаки цифрових слідів, що утворюються під час вчинення кіберзлочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 461. DOI: 10.33994/kndise.2020.65.45 (date accessed: 17.10.2023).

From the point of view of procedural issues, the issue of digital evidence[2] in criminal proceedings should be regulated at legislative level: legislation should contain the procedure for obtaining access to Wi-Fi routers for the purpose of identifying a suspect during inspection, investigation, search and seizure of cybercrimes and performance of other tasks of criminal proceedings. Obtaining access to a Wi-Fi router in a way that is not determined by law can cause a violation of human rights, and according to the *Convention for the Protection of Human Rights and Fundamental Freedom*: "everyone has the right to respect for his private and family life, for his home and correspondence" (Part 1 Article 8) [3]. Since Wi-Fi routers are able to store information about devices that connect to them, including MAC addresses of devices, IP addresses, connection times, information about websites, etc., this information can be used by prosecution to identify a suspect, track movements of such a person and her activity on Internet at the time of committing cybercrime. Therefore, it can be argued that the procedural aspect of the investigation of cybercrimes should contain a clear procedure for the actions of specialists and forensic experts in joint work with pre-trial investigation bodies and procedural manager to obtain evidence of prosecution in criminal proceedings. In addition, data from Wi-Fi routers can be used not only to identify suspects in criminal proceedings during cybercrime investigations: this method can be universal for identifying suspects in criminal proceedings with incomplete data.

Article Purpose

Consider current issues related to identification of suspected cybercrime perpetrators, in particular those using Wi-Fi technology. Investigate possibility of identifying persons suspected of committing cybercrimes who actively hide digital traces of their activities. Analyze the *electronic data* term, as well as the role and specialist participation in such a procedural action as a review in of cybercrime investigation context.

Research Methods

For achieving this goal, general scientific (dialectical, comparison, analysis, synthesis, induction, deduction) and

2 Сіренко О. В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2019. Вип. 14. С. 208—214. DOI: 10.33244/2521-1196.14.2019.208-214 (date accessed: 17.10.2023) ; Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. № 3—2. С. 316—318. URL: https://pap-journal.in.ua/wp-content/uploads/2020/09/3-2_2013.pdf (date accessed: 17.10.2023) ; Алєксєєва-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247—253. URL: http://nvppp.in.ua/vip/2018/2/50.pdf (date accessed: 17.10.2023) ; Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ, 2020. 104 с. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content (date accessed: 17.10.2023).

3 Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) : від 04.11.1950 р.; ратифік. Законом України від 17.07.1997 р. № 475/97-ВР; чинна для України з 11.09.1997 р. (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (date accessed: 17.10.2023).

special scientific methods (formal logical, logical-legal, system-structural ones) were used that contributed to content and validity of scientific conclusions and proposals of this research.

Analysis of Recent Researches and Publications

At the scientific level, the issue of using Wi-Fi routers and information they contain in criminal proceedings not only attracted attention, but became in-depth analysis object by leading scientists and forensic experts. Many scholars and practitioners have devoted their time and efforts to researching this complex issue (particularly in scientific fields such as criminalistics and forensic expertology). Among recent research papers and guidelines on the use of *Wi-Fi* and modern mobile technologies to identify persons suspected of committing criminal offenses, it is possible to distinguish several extremely interesting and promising research papers.

For example, M. Bobets and R. Kobets in 2022 considered investigative team actions in the identification context of person committed a criminal offense, in availability of Wi-Fi router (PC equipment requiring specific expertise) at the scene [4], and suggested using a screenshot of digital evidence concept in criminal proceedings, provided research guidelines that can be used to identify a person who has committed criminal offense. In 2023, M. Kobets investigated the sequence of actions of the investigator, if a mobile terminal (cellular radio telephone) is found at the scene, and the procedure for extracting information (computer data) from this device using the technical capabilities of the *Cellebrite UFED* hardware and software (mentioned research paper deserves attention in the context of logic of case development to establish a suspect in criminal proceedings) [5].

In 2021, V. Polyvoda analyzed the issue of identifying persons involved in commission of crimes using Wi-Fi and provided examples from experience of foreign colleagues [6].

In research guidelines for units of the National Police of Ukraine: *Search and recording of factual data on illegal acts committed using information and telecommunication systems or technologies in the investigation of the facts of sale of narcotics* (2022), the issue of using Wi-Fi to search for persons involved is partially disclosed to illegal circulation of narcotic drugs using the Internet: "under favorable conditions, it is possible to identify such persons, for example, based on the results of viewing the recordings of video surveillance cameras installed in premises where certain areas of Wi-Fi communication were used, where the drug dealer accessed the Internet

4 Кобець М. В., Кобець Р. М. Використання можливостей Wi-Fi роутерів під час виявлення та розслідування кримінальних правопорушень. *Криміналістичний вісник*. 2022. № 2 (38). С. 36—47. DOI: 10.37025/1992-4437/2022-38-2-36 (date accessed: 17.10.2023).

5 Кобець М. В. Дії слідчого під час виявлення на місці події мобільних терміналів (стільникових радіотелефонів). *Там само*. 2023. № 1 (39). С. 52—63. DOI: 10.37025/1992-4437/2023-39-1-52 (date accessed: 17.10.2023).

6 Поливода В. В. Можливості Wi-Fi маршрутизатора у встановленні особи, причетної до вчинення злочину. *Використання досягнень сучасної науки й техніки в розкритті злочинів* : мат-ли міжвідом. наук-практ. кругл. столу (Київ, 25.02.2021). 2021. С. 102—105 / Електронний репозитарій НАВС. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/2f7d687f-7477-4670-80f6-b73c221681dd/content (date accessed: 17.10.2023).

network" [7]. Despite the fact that these recommendations are not aimed at the substantive investigation of cybercrimes, their logical connection with the method of identifying a suspect using Wi-Fi is obvious: they can be useful during the investigation of cybercrimes, although they do not provide for investigation of specific cases of such offenses.

In our opinion, it is worth noting the extremely promising and high-quality guidelines: *Using the capabilities of Wi-Fi routers to install a mobile terminal and its network activity*, prepared in 2022 at the Ukrainian Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine (hereinafter referred to as the *SBU FSISE*) highlighting the theoretical and practical aspects of using a Wi-Fi router which suspect a mobile terminal connected to (this helps to determine the device and its location, as well as network activity, that can indicate a cyberattack) [8]. This publication is intended for employees of forensic expert units, specialists, operatives and investigators.

The guidelines by B. Chernyakhovskyi and V. Yusupov: *Conducting search while investigation of unauthorized access to objects of critical information infrastructure* (2021) [9] deserve attention, because the stage of the general review of the working stage of the search of this publication deserves special attention, and "primary check locations of search objects, including determining type of connection: cable or Wi-Fi" corresponds to the subject of our article's research. In general, these guidelines characterize critical information infrastructure objects and types of criminal attacks on them through unauthorized access, analyze the grounds and procedural procedure for conducting a search and contain forensic recommendations for conducting it during investigation of such crimes and the procedure for conducting investigative actions.

Separately, it is worth mentioning the monograph by O. Samoilenko: Method *fundamentals of the investigation of crimes committed in cyberspace* (2020), which sections are devoted to the forensic characteristics and organization of the investigation of crimes committed in cyberspace [10].

Among the foreign developments, the joint work of Chinese and American scholars in 2012 is of interest, in which it is proposed to classify network forensic investigations into three categories (depending on when law enforcement

7 Кікінчук В. В., Матюшкова Т. П., Піддубна А. В., Манжай О. В., Носов В. В. Пошук та фіксація фактичних даних про протиправні діяння, які вчинені з використанням інформаційно-телекомунікаційних систем або технологій при розслідуванні фактів збуту наркотичних засобів : наук.-метод. рек. для підрозд. Нацполіції Укр. Харків, 2022. 69 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/59910657-34ae-431c-966d-eeaffcb057c8/content (date accessed: 17.10.2023).

8 Нізовцев Ю. Ю. Використання можливостей Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності : метод. рек. Київ, 2022. 18 с.

9 Черняховський Б. В., Юсупов В. В. Проведення обшуку під час розслідування несанкціонованого доступу до об'єктів критичної інформаційної інфраструктури : метод. рек. Київ, 2021. 52 с.

10 Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса, 2020. 372 с. DOI: 10.32837/11300.13264 (date accessed: 17.10.2023).

agencies conduct investigations in response to cybercrime incidents) [11]: in particular, proactive investigations are defined as those that take place to cybercrime incidents; real investigations; those that take place during these incidents, retrospective investigations - those that take place after these incidents. As an example, the application of a portable device based on a smartphone for the real location of a suspect who commits crimes in cyberspace is proposed. This study deals with data collection, GSM and Wi-Fi wireless signal strength and positioning accuracy through experiments.

In addition, in our opinion, by A. Kovalenko in 2017 and 2023 [12] and Ye. Khyzhniak 2017 [13] that investigated specifics of electronic data review a and documents during investigation of criminal offenses. The authors emphasize that in preparation for electronic data review, it is advisable to find out in advance what devices and types of data will have to work with, ensure participation of specialists and availability of the necessary technical means.

Taking into account activity of scientific research in the field of criminalistics based on digital traces and evidence, as well as the available guidelines for the use of Wi-Fi routers for the purposes and tasks of criminal proceedings, it can be confidently stated that the topic of identifying suspects through Wi-Fi routers in investigation of criminal offenses and searches suspects remains extremely relevant. This especially applies to use of modern technologies by criminals to commit crimes in cyberspace. Thereby the use of data from Wi-Fi routers to identify suspects is of particular importance at the stage of pre-trial investigation during investigation of crimes under Sec. XVI (Articles 361-3631) of the Criminal Code of Ukraine [14]. It is important to note that the success of this method of identifying suspects can be of great importance for proving guilt in criminal proceedings, not only during investigation of cybercrimes. Thus, it can be argued that the main purpose of using capabilities of Wi-Fi routers to identify a suspect and subsequently determine the location of radio equipment (radio-electronic means) is not only to establish the suspect location , but to use this data as evidence for prosecution at the stage of pre-trial investigation and legal proceedings.

Academic novelty consists in proposal to supplement part 2 of Art. 71 and Part 7 of Art. 237 of the Criminal Procedure Code

11 Huang J., Chen Yi., Ling Zh., Choo K., Fu X. A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation / UMASS Lowell. #1 Public in mass. Massachusetts Lowell, USA, 2012. 33 p. URL: https://www.uml.edu/docs/HaLo_2012_Fu_tcm18-152079.pdf (date accessed: 17.10.2023).

12 Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України*. 2017. № 1 (88). С. 182—191. URL: http://nbuv.gov.ua/UJRN/vapny_2017_1_19 (date accessed: 17.10.2023) ; Його ж. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки.* 2023. Вип. 4. С. 53—58. DOI: 10.32999/ksu2307-8049/2023-4-9 (date accessed: 17.10.2023).

13 Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право*. 2017. № 4 (58). С. 80—85. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (date accessed: 17.10.2023).

14 Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (date accessed: 17.10.2023).

of Ukraine [15] (hereinafter referred to as Criminal Procedure Code of Ukraine) with information about participation in the review of computer data (on behalf of the investigator, prosecutor and investigator during pre-trial investigation of criminal misdemeanors) by a specialist who has specialized knowledge and understands the process of obtaining electronic data, containing information about MAC addresses from Wi-Fi routers. In addition, it has proper equipment that enables to get digital traces of cybercrime without loss or damage. Based on research paper analysis and normative literature, it can be concluded that, currently there is no clear definition of the *electronic data* term. We offer an expanded interpretation of the concept of *electronic data*, including information contained in Wi-Fi routers. The method of searching for suspects, first proposed by Yu. Nizovtsev which we are considering at the scientific level, can be considered as academic novelty.

Main Content Presentation

Article 84 of Criminal Procedural Code of Ukraine states:

"1. Evidence in criminal proceedings is factual data obtained in the manner prescribed by this Code, on which basis the investigator, prosecutor, investigating judge and the court establish availability or lack of facts and circumstances that are significant for criminal proceedings and subject to proof.

2. Procedural sources of evidence are testimony, material evidence, documents, forensic expert conclusions" [16].

Data from Wi-Fi routers can be one source of evidence. If a suspect was using a Wi-Fi network during the commission of a crime, data about their connection to that network can be used to identify them and further locate them. The data should be understood as the MAC address of the mobile device and other technical data that a specialist or expert can obtain during a search and seizure that involves direct access to the router. Such data can be used to discover connections with other individuals within connections to that network. Taking into account the existing method of identifying suspected persons, which involves the use of data on the connection of a mobile device to Wi-Fi routers, it is necessary to consider problematic issues that contain a possible change of data on a connected mobile device in order to hide it. One of problematic issues in investigation of a cybercrime is concealment of information during its commission. Such concealment occurs by replacing or cloning the MAC address of the mobile device with the standard software of this device. MAC address (*Media Access Control*) is a unique identifier for a network interface. In the OSI (*Open Systems Interconnection model*) network model, the MAC address is used at the second (channel) level. Sometimes this address is called hardware or physical (*Hardware Address*). The MAC address of network interface is provided by the manufacturer, while the address space is distributed among manufacturers. Changing the MAC address can make it conditionally impossible to identify a mobile device based on data about its connection to Wi-Fi routers. Another problematic issue is the possibility of using a VPN. A VPN connection creates an encrypted channel between a mobile device and a VPN server, allowing hide data about network activity of a mobile device connected to a Wi-Fi network,

15 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 17.10.2023).

16 Ibidem.

but without hiding MAC address data. Therefore, ability to identify the mobile terminal remains (if MAC addresses have not been changed), although the signs of a cyberattack (type of attack, its goal, etc.) can be hidden. Another problematic issue is possibility of using special software tools to disguise a mobile device as another device i.e., deliberately changing the MAC address not to an arbitrary address, but to the address of another specific mobile device in order to compromise it. These problematic issues can make it difficult or impossible to apply existing method of identifying suspects, so they need to be solved immediately.

In the above-mentioned guidelines: *Using capabilities of Wi-Fi routers to establish a mobile terminal and its network activity*, developed by SBU FSISE, it is stated that "use of information about connected mobile terminals recorded by the Wi-Fi router is possible if the router supports logging of network connections and if such logging is activated" [17]. In other words, information characterizing mobile terminals directly connected to the Wi-Fi network usually contains data about the network name of such a terminal, its MAC address, IP address, network connection time and session duration. Using reference data, the manufacturer of the mobile terminal can usually be determined by the MAC address, and in some cases, the specific model. In these guidelines, problematic issues of identification of suspected persons are also raised: "Certain features of the MAC address should be taken into account. First, this address can be changed in the settings of the mobile terminal or using special software. For example, modern smartphones have the function of generating a random MAC address every time you connect to network <...>. Second, the MAC address is not transmitted globally with network traffic. Within the Wi-Fi network, the MAC address is transmitted from the terminal only to the router, not further. And therefore, it is usually impossible to track a mobile terminal by its MAC address in global network" [18].

V. Polyvoda in the above-mentioned research paper notes that "in order to use the capabilities of the Wi-Fi router, it is necessary to understand that it is possible to change the MAC address on the technical device itself. Its change occurs only if the smartphone is not currently connected to any Wi-Fi network. With the help of special algorithms, it can be detected and filtered on the device with 100 % certainty. In particular, in addition to the random MAC address, smartphones periodically send the correct MAC address, which receives the Wi-Fi radar." The scientist notes that "share of smartphones that can replace their MAC address is no more than 30 % of large cities" [19].

M. M. Kobets and R. Kobets noted that "investigator (operative), on the basis of the decision of examining magistrate of the court of first instance, sends a request to the network operators of cellular radiocommunication in order to verify the MAC addresses established during the inspection of the scene and to establish the user data (IMEI, phone numbers and other data) that are in the database system of the provider of electronic

17 Нізовцев Ю. Ю. Op. cit.
18 Ibidem.
19 Поливода В. В. Op. cit. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/2f7d687f-7477-4670-80f6-b73c221681dd/content (date accessed: 17.10.2023).

communication services of cellular radio communication" [20]. This algorithm application is primarily hampered by the fact that cellular operators do not have information about the MAC addresses of mobile terminals, so they are not able to provide such information at the investigator request, even if such a request is made in compliance with all procedural requirements.

Cellular operators receive information about mobile devices using their network, in particular IMEI (*International Mobile Equipment Identity*) numbers of these devices, as well as the subscriber identifier IMSI (*International Mobile Subscriber Identity*) contained in a SIM/USIM/R-UIM card. In most cases, the MAC address is used to identify a mobile device on a Wi-Fi network, not on a mobile network. In addition, "IMEI and IMSI are unique numbers. IMEI is provided to the mobile terminal by its manufacturer, IMSI by manufacturer of the SIM/USIM/R-UIM card, usually by the cellular operator (by the factory on its order). Therefore, the manufacturer of the mobile terminal has information about as IMEI (tracked by cellular operators) as MAC address of the terminal. This can be used when searching for a mobile terminal" [21]. Procedural procedure for searching for a mobile terminal is stipulated in Criminal Procedural Code of Ukraine, besides, such a search has its own special technical specifics.

In this regard, we suggest to "*install through reference sources on the Internet the terminal manufacturer that has the detected MAC address. Note that if the exact model of the terminal can usually be determined by the IMEI in reference Internet sources, then only the manufacturer can be determined by the MAC address. Having information about the manufacturer of the mobile terminal, in certain cases, it is possible to preliminarily assume what kind of device; it was smartphone, tablet computer, laptop, separate network interface (card), etc.*" [22]. Thus, first of all, you should establish the manufacturer of the terminal by its MAC address, but this can only give general information about the manufacturer. To obtain such information, it is necessary to contact the manufacturer, especially if this company manufactures different types of devices (i.e., in addition to Wi-Fi, the mobile terminal may have a built-in 3G/4G modem with which the mobile terminal can connect to the cellular network). Having determined the manufacturer based on the MAC address data, it is possible to contact the mobile terminal manufacturer for information about the IMEI of such a terminal. Then it is possible to get subscriber data, traffic data, connection duration, calls, etc. One of the forms of obtaining such data is a request from an investigator, in accordance with Art. 93 of the Criminal Procedural Code of Ukraine [23], according to the decision of the investigating judge, to cellular radio operators for the purpose of checking IMEI and setting user data in the database system of the provider of electronic communication services. After receiving the requested data from the cellular operator, the investigator,

20 Кобець М. В., Кобець Р. М. Op. cit. DOI: 10.37025/1992-4437/2022-38-2-36 (date accessed: 17.10.2023).

21 Нізовцев Ю. Ю. Op. cit.

22 Ibidem.

23 Кримінальний процесуальний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 17.10.2023).

the prosecutor may decide to conduct such an undercover investigative (search) action as establishing the location of radio equipment (radio-electronic means) in accordance with Art. 268 of Criminal Procedural Code of Ukraine of Ukraine [24]. It is premature to talk about the effectiveness of such procedural actions based on the data received from the cellular operator. Effectiveness of procedural actions based on information received from the mobile operator will later affect the results of investigative practice. At the same time, it is necessary to take into account all the peculiarities of the collection of evidence by specialists, importance of such information for the identification of suspects, all procedural aspects of making procedural decisions and efficiency of their implementation, as well as the complexity of criminal proceedings in general. Initial evidence collection is very important, which will directly affect as beginning of the pre-trial investigation in particular as criminal proceedings in general. Effectiveness of the substantive criminal proceedings and the role of the specialist in gathering evidence that can be obtained from Wi-Fi routers acquire special importance in view of some circumstances. The parties to criminal proceedings (during the pre-trial investigation) and court (during the trial) may engage a specialist to provide technical assistance (photographing, drawing up diagrams, plans, drawings, sampling samples for examination, etc.), as well as to provide opinions in cases, provided for in Clause 7, Part 4 of Art. 71 of Criminal Procedural Code of Ukraine (according to part 2 of this article). The specialist is obliged to come upon summons to the investigator, inquirer, prosecutor, court and have with him the necessary technical equipment, devices and instruments (clause 1, part 5, article 71 of the Criminal Procedure Code of Ukraine) [25]. Therefore, specific expertise of specialist and availability of technical equipment, devices and devices can help the investigator, prosecutor and inquirer during the pre-trial investigation of criminal offenses to obtain primary evidence of the prosecution from the Wi-Fi router in order to identify the suspect person or group of persons and establish their location.

Taking into account the fact that specialist's knowledge and experience (in the case of participation in the review, search and provision of technical assistance during investigation of cybercrimes) can be of decisive importance for prosecution, it is advisable to consider the possibility of making changes to Art. 71 and 237 of the Criminal Procedural Code of Ukraine [26] regarding expansion of the powers of a specialist in criminal proceedings to examine electronic data and clarifying the interpretation of the *electronic data* term (in the context of regulating procedure for examining network equipment by specialist for the purpose of identifying mobile devices of suspects based on MAC addresses data, IMEI and IMSI). The purpose of such changes is to create clearer and more detailed procedural requirements for the review of such investigations. However, first it is necessary to analyze the *electronic data* term.

24 Кримінальний процесуальний кодекс України ... . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 17.10.2023).
25 Ibidem.
26 Ibidem.

As early as 2007, Ye. Rashchenko noted that "there is a widespread opinion among many scientists; it is possible to influence computer information only with the help of other computer information. Based on this thesis, they note that mandatory feature of *cybercrimes* is such an instrument of their commission as computer information. <...> It should also be understood that computer data can either directly act as traces of a crime or contain such traces" [27] and referred to V. Holubiev: "Considering computer data as a source of forensic information, one cannot ignore the issue of its direct seizure. Such seizure may be carried out during a search, inspection of the scene, seizure or even reproduction of the situation and case circumstances" [28].

O. Kravchuk drew attention to problematic issues related to the *electronic data* definition and noted that "although there is currently no definition of computer data, the question may arise as to whether the contents of the seized phone should be reviewed as a review of computer data or as overview of things" [29]. Regarding the changes to the Criminal Procedural Code of Ukraine, the author notes the following: "Addition to Art. 237 of the Criminal Procedural Code of Ukraine stipulates that the investigator and the prosecutor can conduct an inspection not only of the area, premises, things and documents, but also of computer data" [30].

Analysis of scientific literature and legislative framework indicates that to date there is no definition of *electronic data* term and electronic data review is carried out by the investigator, prosecutor: "by reflecting in the review protocol the information they contain in a form suitable for perceiving their content (by electronic means, photography, video recording, shooting and/or video recording of the screen, etc., or in paper form)" (paragraph 2 of Part 2 of Article 237 of Criminal Procedural Code of Ukraine)[31]. It is also necessary to agree with O. Kravchuk on the features of inspection of the phone for electronic data that should be separated from a simple inspection of things.

We propose to expand the interpretation of *electronic data* term. Since the information located in Wi-Fi routers can contain MAC addresses of mobile devices of persons suspected of committing cybercrime (i.e., various mobile devices: smartphones, tablets, laptops, etc.), this information can be considered as electronic data. In such a case, an inspection or search of the contents of a phone or Wi-Fi router to identify factual data that can be of interest during the investigation of cybercrime can be classified as an inspection or search of computer data, provided that, in procedural terms, prosecution can still use them as evidence.

Returning to the issue of procedural significance of the review, it should

27 Ращенко Є. Комп'ютерні дані як носій криміналістичної інформації про злочин у сфері комп'ютерних технологій. *Правова інформатика*. 2007. № 1. С. 76—80. URL: http://nbuv.gov.ua/UJRN/Pinform_2007_1_12 (date accessed: 17.10.2023)

28 Голубєв В. О. Комп'ютерні злочини в банківській діяльності. Запоріжжя, 1997. С. 125.

29 Кравчук О. «Обшук» мобільних телефонів і комп'ютерів та інші зміни до КПК / Вищий антикорупційний суд України : офіц. сайт. Новини та події. 24.03.2022. URL: https://first.vaks.gov.ua/publications/37254/ (дата звернення 17.10.2023).

30 Ibidem.

31 Кримінальний процесуальний кодекс України ... . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 17.10.2023).

be noted that according to Part 1 and Paragraph 1 of Part 2 of Art. 237 of the Criminal Procedural Code of Ukraine of Ukraine, the investigator and the prosecutor conduct computer data review, namely:

"1. In order to identify and record information about circumstances of criminal offense commission, the investigator and prosecutor conduct an inspection of the area, premises, things, documents and electronic data.

2. Inspection of a person's home or other property is carried out in accordance with the rules of this Code, provided for the search of a person's home or other property" [32].

Paragraph 2 of Part 6 of Art. 236 of Criminal Procedural Code of Ukraine provides additional features for the search, detection and recording of computer data during the search: "If during search and seizure the investigator, the prosecutor found access or the possibility of access to computer systems or parts thereof, mobile terminals of communication systems, for the detection of which no permission was granted to conduct a search, but for which there are sufficient grounds to believe that the information contained therein is important for establishing the circumstances in the criminal proceedings, the prosecutor, the investigator has the right to search, detect and record electronic data contained therein at the search and seizure location" [33].

However, it is worth emphasizing importance of review as a procedural procedure that plays a key role in collecting initial digital traces of cybercrime. In this case, the statement that review can be as forensic as procedural action can be considered, acquiring a new, independent meaning, especially if considering a specialist who can help obtain such electronic data during review procedure, in the manner established by Criminal Procedural Code of Ukraine. According to Part 7 of Art. 237 of Criminal Procedural Code of Ukraine: "during the inspection, the investigator, the prosecutor or the specialist involved on their behalf has the right to take measurements, take photographs, make sound or video recordings, draw up plans and diagrams, make graphic images of the inspected place or individual items, make impressions and casts, inspect and seize things and documents relevant to criminal proceedings. Items that are withdrawn from circulation by law are subject to withdrawal regardless of their relation to criminal proceedings. Confiscated things and documents that are not related to items that have been withdrawn from circulation by law are considered temporarily confiscated property" [34]. At the same time, this norm does not contain specialist actions regarding electronic data review data on behalf of an investigator, a prosecutor. Participation of specialist in the cybercrime aftermath and during electronic data review is important, and in some cases simply necessary, because the specialist: "has specific expertise and skills and can provide advice, explanations, references and conclusions during pre-trial investigation and trial with issues requiring relevant specific expertise and skills" (Part 1 of Article

32 Кримінальний процесуальний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 17.10.2023).

33 Ibidem.

34 Ibidem.

71 of the Criminal Procedure Code of Ukraine) [35].

Conclusions

We propose to amend Part 2 of Article 71 of the Criminal Procedure Code of Ukraine as follows: *"A specialist may be engaged to provide direct technical assistance (photographing, drawing up diagrams, plans, drawings, sampling for examination,* ***conducting a review of electronic data****, etc.) to the parties to criminal proceedings during pre-trial investigation and hearing, as well as to provide conclusions in the cases provided for in paragraph 7 of part four of this article"*.

Taking into account the above, to Part 7 of Art. 237 of Criminal Procedural Code of Ukraine needs to be amended to provide for participation of specialist during electronic data review on behalf of the investigator, prosecutor and investigator during the pre-trial investigation of criminal misdemeanors. A specialist not only has the special knowledge and understanding of how to properly obtain electronic data from Wi-Fi router, which will include information about MAC addresses: he has the necessary technical equipment, devices and instruments that can contribute to obtaining digital traces committing a cybercrime without losing or corrupting such data. Therefore, we propose to set out Part 7 of Art. 237 of Criminal Procedure Code of Ukraine in the following wording: *"During inspection, the investigator, the prosecutor or specialist* ***involved on their behalf*** *has the right to measure, photograph, sound or video record,* ***search, identify and record electronic data****, draw up plans and schemes, make graphic images of the inspected location or individual items, make prints and casts, inspect and seize items and documents relevant to criminal proceedings. Items that are withdrawn from circulation by law are subject to withdrawal regardless of their relation to criminal proceedings. Confiscated things and documents that do not belong to items that have been withdrawn from circulation by law are considered temporarily confiscated property"*.

Summarizing analysis of the *electronic data* term, we come to the following conclusion: *"****electronic data*** *is information contained in Wi-Fi routers, as well as actual data on MAC addresses, IMEI and IMSI of mobile devices, which the prosecution can use to search for a suspect or a group of persons in order to prosecute them"*. We consider it appropriate to apply the provisions and conclusions of this author's research on crime detection and investigation, investigative and forensic expert activities.

Установлення особи, підозрюваної у скоєнні кіберзлочину з використанням *WiFi*-технологій

Юрій Нізовцев, Олег Парфило, Олег Плахотнік

Мета статті — дослідити питання використання WiFi-маршрутизаторів та інформації, яку вони містять, під час розслідування кіберзлочинів, учинених із використанням WiFi-технології, як методу, ефективного для встановлення підозрюваної особи або групи осіб з подальшим визначенням місця їх знаходження. Для досягнення поставленої мети застосовано загальнонаукові та спеціальні наукові методи дослідження. Опрацьовано різні методичні рекомендації щодо використання WiFi-маршрутизаторів для встановлення мобільного пристрою шляхом судово-експертного дослідження.

35 Кримінальний процесуальний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 17.10.2023).

Наголошено, що в разі скоєння кіберзлочину із застосуванням WiFi-маршрутизатора, спеціаліст та експерт можуть використати технічну інформацію з WiFi-маршрутизатора для ідентифікації мобільного пристрою підозрюваної особи за MAC-адресою. Розглянуто проблемні питання із виявлення ознак приховування цифрових слідів під час скоєння кіберзлочину. Викладено процесуальний порядок отримання доступу до WiFi-маршрутизаторів із метою встановлення підозрюваної особи під час огляду, обшуку й розслідування кіберзлочинів. Доведено, що дані з WiFi-маршрутизаторів сприятимуть не тільки встановленню підозрюваних осіб у кримінальних провадженнях під час розслідування кіберзлочинів: цей метод може виявитися універсальним для встановлення підозрюваних осіб у кримінальних провадженнях із неповними даними. Проаналізовано термін «комп'ютерні дані», відзначено особливу роль спеціаліста у проведенні огляду комп'ютерних даних і запропоновано змінити чинний Кримінальний процесуальний кодекс України в частині участі спеціаліста в огляді комп'ютерних даних за дорученням слідчого, прокурора й дізнавача під час досудового розслідування кримінальних проступків. Положення та висновки авторського дослідження стануть у пригоді в оперативно-розшуковій, слідчій і судово-експертній діяльності.

Ключові слова: *кіберзлочини; маршрутизатори; WiFi-технології; електронні комунікації; електронні докази; цифрові сліди; розслідування; судова експертиза; методичні рекомендації.*

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

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

Participants
Authors contributed solely to the intellectual discussion underlying this document, case law research, writing and editing and assumes responsibility for its content and interpretation.

Declaration of Competing Interest
The authors declares no conflict of interest.

References

Alieksieieva-Protsiuk, D. O., Bryskovska, O. M. (2018). Elektronni dokazy v kryminalnomu sudochynstvi: poniattia, oznaky ta problemni aspekty zastosuvannia [Electronic evidence in criminal justice: concepts, characteristics and problematic aspects of application]. *Naukovyi visnyk publichnoho ta pryvatnoho prava.* Vyp. 2. URL: http://nvppp.in.ua/vip/2018/2/50.pdf [in Ukrainian].

Cherniakhovskyi, B. V., Yusupov, V. V. (2021). Provedennia obshuku pid chas rozsliduvannia nesanktsionovanoho dostupu do obiektiv krytychnoi informatsiinoi infrastruktury [Conducting search during investigation of unauthorized access to objects of critical information infrastructure] : metod. rek. Kyiv [in Ukrainian].

Holubiev, V. O. (1997). Kompiuterni zlochyny v bankivskii diialnosti [Computer crimes in banking]. Zaporizhzhia [in Ukrainian].

Huang, J., Chen, Yi., Ling, Zh., Choo, K., Fu, X. (2012). *A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation* / UMASS Lowell. #1 Public in mass. Massachusetts Lowell, USA. URL: https://www.uml.edu/docs/HaLo_2012_Fu_tcm18-152079.pdf.

Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H. ta in. (2020). Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh [Use of digital evidence in criminal proceedings] : metod. rek. / za zah. red. O. V. Korneika. Vyd. 2-he, dop. Kyiv. URL: https://elar.naiau.kiev.ua/server/api/core/

bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content [in Ukrainian].

Khyzhniak, Ye. S. (2017). Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen [Peculiarities of reviewing electronic documents during investigation of criminal offenses]. *Derzhava ta rehiony. Seriia: Pravo.* № 4 (58). URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf [in Ukrainian].

Kikinchuk, V. V., Matiushkova, T. P., Piddubna, A. V., Manzhai, O. V., Nosov, V. V. (2022). *Poshuk ta fiksatsiia faktychnykh danykh pro protypravni diiannia, yaki vchyneni z vykorystanniam informatsiino-telekomunikatsiinykh system abo tekhnolohii pry rozsliduvanni faktiv zbutu narkotychnykh zasobiv* [Search and recording of factual data on illegal acts committed using information and telecommunication systems or technologies while investigating facts of sale of narcotic drugs] : nauk.-metod. rek. dlia pidrozd. Natspolitsii Ukr. Kharkiv. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/59910657-34ae-431c-966d-eeaffcb057c8/content [in Ukrainian].

Kobets, M. V. (2023). Dii slidchoho pid chas vyiavlennia na mistsi podii mobilnykh terminaliv (stilnykovykh radiotelefoniv) [Investigator's actions during detection of mobile terminals (cellular radiotelephones) at the scene]. *Kryminalistychnyi visnyk.* № 1 (39). DOI: 10.37025/1992-4437/2023-39-1-52 [in Ukrainian].

Kobets, M. V., Kobets, R. M. (2022). Vykorystannia mozhlyvostei Wi-Fi routeriv pid chas vyiavlennia ta rozsliduvannia kryminalnykh pravoporushen [Using capabilities of Wi-Fi routers in detection and investigation of criminal offenses]. *Kryminalistychnyi visnyk.* № 2 (38). DOI: 10.37025/1992-4437/2022-38-2-36 [in Ukrainian].

Kovalenko, A. V. (2017). Osoblyvosti taktyky ohliadu elektronnykh dokumentiv pid chas dosudovoho rozsliduvannia posiahan na zhyttia ta zdorovia zhurnalista [Features of the tactics of reviewing electronic documents during the pre-trial investigation of attacks on the life and health of a journalist]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy.* № 1 (88). URL: http://nbuv.gov.ua/UJRN/vapny_2017_1_19 [in Ukrainian].

Kovalenko, A. V. (2023). Orhanizatsiia i taktyka provedennia ohliadu kompiuternykh danykh [Management and tactics of electronic data review]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia: Yurydychni nauky.* Vyp. 4. DOI: 10.32999/ksu2307-8049/2023-4-9 [in Ukrainian].

Kravchuk, O. (2022). *«Obshuk» mobilnykh telefoniv i kompiuteriv ta inshi zminy do KPK* [Search and seizureof mobile phones and computers and other changes to Criminal Procedural Code of Ukraine] / Vyshchyi antykoruptsiinyi sud Ukrainy : ofits. sait. Novyny ta podii. 24.03.2022. URL: https://first.vaks.gov.ua/publications/37254/ [in Ukrainian].

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

Nizovtsev, Yu. Yu. (2022). *Vykorystannia mozhlyvostei Wi-Fi marshrutyzatoriv dlia vstanovlennia mobilnoho terminalu ta yoho merezhevoi aktyvnosti* [Using the capabilities of Wi-Fi routers to install a mobile terminal and its network activity] : metod. rek. Kyiv [in Ukrainian].

Omelian, O. S. (2020). Poniattia ta oznaky tsyfrovykh slidiv, shcho utvoriuiutsia pid chas vchynennia kiberzlochyniv [Concepts and features of digital traces formed during the commission of cybercrimes]. *Kryminalistyka i sudova ekspertyza.* Vyp. 65. DOI: 10.33994/kndise.2020.65.45 [in Ukrainian].

Polyvoda, V. V. (2021). Mozhlyvosti Wi-Fi marshrutyzatora u vstanovlenni osoby, prychetnoi do vchynennia zlochynu [Possibilities of a Wi-Fi router in establishing the person involved in the commission of a crime]. *Vykorystannia dosiahnen suchasnoi nauky y tekhniky*

v rozkrytti zlochyniv : mat-ly mizhvidom. nauk-prakt. kruhl. stolu (Kyiv, 25.02.2021) / Elektronnyi repozytarii NAVS. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/2f7d687f-7477-4670-80f6-b73c221681dd/content [in Ukrainian].

Rashchenko, Ye. (2007). Kompiuterni dani yak nosii kryminalistychnoi informatsii pro zlochyn u sferi kompiuternykh tekhnolohii [Computer data as a carrier of forensic information about a crime in the field of computer technology]. *Pravova informatyka.* № 1. URL: http://nbuv.gov.ua/UJRN/Pinform_2007_1_12 [in Ukrainian].

Samoilenko, O. A. (2020). *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori* [Fundamentals of Methods for Investigating Crimes Committed in Cyberspace] : monohrafiia / za zah. red. A. F. Volobuieva. Odesa. DOI: 10.32837/11300.13264 [in Ukrainian].

Sirenko, O. V. (2019). Elektronni dokazy u kryminalnomu provadzhenni [Digital evidence in criminal proceedings]. *Mizhnarodnyi yurydychnyi visnyk: aktualni problemy suchasnosti (teoriia ta praktyka).* Vyp. 14. DOI: 10.33244/2521-1196.14.2019.208-214 [in Ukrainian].

Nizovtsev, Yu., Parfylo, O., Plakhotnik, O. (2023). Identification of Person Suspected of Committing a Cybercrime Using Wi-Fi Technologies. *Theory and Practice of Forensic Science and Criminalistics.* Issue 4 (33). P. 23—38. DOI: 10.32353/khrife.4.2023.03.