https://doi.org/10.15407/scine21.06.060

AHARKOVA, O. I. [1] (https://orcid.org/0000-0002-6236-4198),
KOROSTELEVA, L. A. [2] (https://orcid.org/0000-0002-4782-1354),
and KRASNOPOLSKYI, V. E. [3] (https://orcid.org/0000-0002-1413-2747)

[1] Investigative Department of the Main Directorate
of the National Police in Kharkiv Region,
14, Vesnina St., Kharkiv, 61023, Ukraine,
+380 57 730 8907, kh_su@hk.police.gov.ua
[2] Ministry of Internal Affairs of Ukraine,
10, Akademika Bohomoltsia St., Kyiv, 01032, Ukraine,
+380 44 256 0072, pgmia@mvs.gov.ua
[3] Dnipro State University of Internal Affairs,
26, Nauky Ave., Dnipro, 49005, Ukraine,
+380 56 756 4545, info@dduvs.edu.ua

THE USE OF INNOVATIVE SOFTWARE PACKAGES IN DIGITAL FORENSICS TO COMBAT CRIME IN UKRAINE

Introduction. *Digital forensics, based on the application of specialized software packages, has significantly enhanced the efficiency of criminal investigations. Mobile devices have become integral to the daily lives of both citizens and offenders, creating new challenges for law enforcement agencies.*

Problem Statement. *The growing number of criminal offenses involving mobile devices has required the deployment of specialized tools capable of extracting and analyzing large volumes of data stored on these devices that subsequently serve as critical evidence in criminal proceedings.*

Purpose. *The purpose of this article is to develop practical recommendations grounded in an analysis of the practical use of advanced software packages and the generalization of studies on seized digital evidence, aimed at strengthening the use of innovative software tools in digital forensics to support the fight against crime in Ukraine.*

Materials and Methods. *The study has examined the capabilities of UFED, Oxygen Forensic Detective, XRY, and EnCase Mobile Investigator. A comparative analysis of these tools has been conducted using data from real criminal cases. In addition, expert interviews with digital forensics professionals have provided supplementary insights into the practical application of these software packages.*

Results. *The advantages of each software package for mobile forensics have been identified. The UFED (Universal Forensic Extraction Device) platform has been shown to be the primary tool used by Ukrainian law enforcement agencies. Its application has significantly reduced the time required for data collection and analysis, improved the accuracy and reliability of extracted evidence, and increased the overall detection rate of offenses.*

Conclusions. *The integration of innovative digital forensic technologies into law enforcement practices has contributed to more effective pre-trial investigations of crimes involving mobile devices. The recommendations developed in this study have offered valuable guidance for enhancing the practical activities of law enforcement officers in Ukraine.*

Keywords: digital forensics, digital evidence, software packages, UFED (Universal Forensic Extraction Device), Oxygen Forensic Detective, crime.

Citation: Aharkova, O. I., Korosteleva, L. A., and Krasnopolskyi, V. E. (2025). The Use of Innovative Software Packages in Digital Forensics to Combat Crime in Ukraine. *Sci. innov.*, 21(6), 60—67. https://doi.org/10.15407/scine21.06.060

At present, every person uses several mobile devices (cell phones, smartphones, tablets, etc.) daily and also has access to a large number of digital services. The capabilities and the number of users of these devices are growing every year. According to statistics from DataReportal, We Are Social, and Meltwater, published in the annual Digital 2024 report, there were 5.61 billion mobile device users at the beginning of 2024, which is 69.4% of the total world population. In addition, this indicator has increased by 138 million (+2.5%) over the past year [1]. In everyday life, this has led to the accumulation of extensive digital footprints, thereby increasing the likelihood that such traces will be left in the event of a crime. In turn, the need for law enforcement agencies for effective tools for detecting, extracting, and investigating digital footprints is constantly growing, and this area is one of the most relevant in forensic science.

Electronic (digital) information as an integral attribute of modern criminal and forensic activities determines the prospects for the development of forensics, which are associated with the revision of both individual components of its system and forensics as a whole, and determines the prospects for further scientific research in this line of investigation [2].

The term "computer forensics" was first used in scientific literature by R. Sommer and M. Goodman in the article "Computers and Law: the Use of Computers in British Criminal Investigations" [3], which became the precursor and synonym of digital forensics [4]. R. Mohanakrishnan also believes that the terms "digital forensics," "computer forensics" and "cyber forensics" can be used synonymously [5]. However, the American scientist and industry expert M. Sheetz points out that this area of forensic science deals with the investigation of computer crimes, counteracting their commission, and how computers can be used to investigate, prosecute and prevent these crimes [6]. In turn, P. Reedy specified the current areas of digital forensics: 1) research of cloud storage; 2) research of mobile devices (phones); 3) research of programs (messengers and other applications for smartphones used for information exchange); 4) research of Internet of Things (IoT); 5) network research; 6) research of the latest devices and applications (Alexa from Amazon, Google Assistant, Siri from Apple, etc.); 7) research of applications not for the phone (research of databases, Spotlight, America online instant messaging, drones, volatile memory, Darknet, anti-forensic tools, deleted and fragmented files, images, flash memory, cryptocurrencies); 8) digital behavior analysis; 9) digital forensic intelligence and open source intelligence, etc [7].

Domestic scientists A. Kolodina and T. Fedorova define digital forensics as an applied science "about solving crimes related to computer information, about the study of digital evidence, methods of searching, obtaining, and securing such evidence" [8]. In turn, R. Stepaniuk and S. Perlin consider digital forensics to be a separate branch of forensic science, representing a system of scientific methods for the study of digital evidence to assist in the detection and investigation of criminal offenses [9].

As mentioned above, neither Ukrainian scientists nor scientists from many countries of the world have reached a consensus on the interpretation of the concept of "digital forensics" and the systematization of its means and methods, but it should be noted that this field is primarily forensic. In modern criminal investigation methods, significant efforts are being made to integrate the technical aspects of digital evidence research to ensure a quick, complete and unbiased investigation.

The role of a digital crime investigator involves searching for evidence on seized equipment using specialized tools. Access to digital traces shall be obtained legally, following criminal procedural law. This can include acquiring computers or data carriers as per Article 93(2) of the Ukrainian Code of Civil Procedure of Ukraine (CPC), gaining temporary access via a judge's decision, or seizing items during investigative actions.

Thus, the Android OS and platform on mobile devices enable intricate communication services online. This allows users to exchange various forms of data such as text, voice, audio, video, images, and

more through different applications. However, these advanced features and technologies can also be exploited by wrongdoers for criminal activities like cyberbullying, email scams, child exploitation, drug-related communication, etc. [10].

Numerous research has been conducted on data extraction methods from diverse mobile devices employing both open-source and proprietary digital forensics tools. These methodologies have become firmly established within forensic laboratories for information retrieval. In 2018, Umar R., Riadi I., and Zamroni G. M. have conducted a comprehensive analysis of the WhatsApp messenger database, which utilizes crypt12 encryption, employing the Belkasoft Evidence and WhatsApp Key/DB Extractor software suites. WhatsApp Key/DB Extractor demonstrated superior efficacy in extracting text messages, while Belkasoft Evidence yielded significantly better results in extracting media and documents [11].

Oluwasetemi Osho and Ohida S.O. evaluated mobile forensic tools, namely AccessData FTK, EnCase, MOBILedit Forensic Express, and Oxygen Forensic Suite, on two mobile devices named HTC Desire 300 with Android v4.1.2 and Samsung Galaxy GT-S5300 with Android v2.3.5, focusing on deleted data recovery. They concluded that FTK and EnCase outperformed MOBILedit and Oxygen Forensic Suite in data recovery. In addition to WhatsApp applications, other applications on mobile devices have been analyzed using Android Studio and DB browser through logical and physical data acquisition, where the two aforementioned software packages were successful [12].

Digital forensics operate on the basis of logical, physical, and file system data extraction tools. The examination of evidence involves a broad array of tools, both commercial and open-source. This field follows the international standard DSTU ISO/IEC 27037:2017 Information Technology. Security Techniques. Guidelines for the Identification, Collection, Acquisition, and Preservation of Digital Evidence (ISO/IEC 27037:2012, IDT) in Ukraine. The selection of methods is largely influenced by the mobile device's operating system and tool capabilities. Prior to extracting evidence from a mobile device, specialists need details about the device model and the operating system's security patch level.

It is also worth noting that at present, there are more than 20 expert methods registered in Ukraine in the speciality 10.9 "Research of computer equipment and software products," most of which have been developed by specialists of forensic institutions of the Ministry of Justice of Ukraine. However, the extremely rapid update of tools and software in the field of information technology leads to the rapid obsolescence of methods of forensic analysis [13].

Currently, it is important to constantly improve and update the methodology of mobile device forensic analysis to meet modern requirements and technological realities in the field of computer and software expertise. The development of new methodologies, tools, and approaches to working with digital evidence is a key component of the development of digital forensics, which shall adapt to the dynamically changing digital environment. It is precisely the consideration of the features of the application of digital forensics, and the highlighting of key problematic aspects that arise both among theorists and practitioners in this field, that we consider it expedient to address in this publication.

METHODOLOGY FOR CONDUCTING A MOBILE DEVICE INVESTIGATION

In the mobile device research methodology, it is possible to logically extract data without physically connecting to the device. This process uses a third-party application that collects data on the device itself. Connection to the application is possible through OTG connection technology or wireless communication. In the case of iOS technology, the latest version can be partially jailbroken by exploiting device vulnerabilities. To install specialized firmware and check the compatibility of a sample mobile device, an online check is performed using the IMEI number on the website https://www.imei.info/ [14].

During the pre-trial investigation, specialists, using a specialized certified tool, such as the UFED (Universal Forensic Extraction Device) software complex, extract information from mobile devices: the phone book with a list of saved phones, phone calls, including SMS, MMS with the date and duration of calls with the indication of subscribers. Before collecting data, the compatibility of the mobile device sample with all possible tools is checked. For testing, a mobile device with the latest version of the Android operating system and the current level of security updates is used to analyze the performance of the tool. The first step includes isolating the mobile device, activating airplane mode and developer mode, and disabling automatic screen lock. After setting up the location of the corresponding mobile device model, the process of connecting the mobile terminal to a specific data collection tool using physical extraction begins. At the final stage of data collection, the mobile device is switched to download mode.

It is important to note that Ukrainian law prescribes a specific procedure for obtaining such information. Notably, Article 264 of the CPC addresses the retrieval of information from electronic information systems. Additionally, Chapter 21 of the CPC governs the conduct of covert investigative (detective) actions that may be relevant to securing this information.

It should also be noted that quite often the owner of a mobile phone sets up pattern lock protection with various keys set in the form of a pattern of numbers, graphics, or biological identification by fingerprint. Thus, in order to check whether these tools were able to bypass or crack the pattern lock, and the type of technique they use, there is a need to connect to a special mode that removes the lock.

Ensuring the comprehensiveness and integrity of extracted data from mobile devices is paramount. While logical data recovery methods can provide some information, such as phonebook entries, photos, videos, browser history, and email, they may not capture the full scope of relevant data. In cases where deleted information is crucial, employing file system collection methods is often a more effective approach.

Based on the results of research and work with such software packages as UFED (Universal Forensic Extraction Device), Oxygen Forensic Detective, XRY, EnCase Mobile Investigator, we have determined that they collect almost all deleted information from a mobile device by extracting information from the file system. The process of collecting information using these software packages is the same as the process of logically unloading data from a mobile device, but there is a certain discrepancy that lies in the use of the Android operating system debugging mode. There are partitions that an ordinary user does not have access to during the setup process, and that are specially created for developers. The Android operating system debugging mode, also known as ADB, is used by developers to support software. Additionally, automatic physical data extraction is performed, which is a bit-by-bit copy that includes not only allocated data, but also all unallocated data, where deleted files may be present. This allows finding hidden or deleted information on mobile devices. File parsing is a well-known method of data disclosure. It also enables restoring deleted or hidden data on the storage device.

ANALYSIS OF THE STUDY OF SOFTWARE PACKAGES

The arsenal of scientific and technical means and methods of forensics is constantly enriched by integrating the most significant achievements of scientific and technological progress and purposeful development of technical and forensic means and technologies, techniques and methods aimed at meeting the current and future needs of investigative, expert, judicial, operational, law enforcement and human rights practice.

Currently, two software packages UFED (Universal Forensic Extraction Device) and Oxygen Forensic Detective are in use in Ukraine, both of which are in high demand among experts and law enforcement agencies.

The UFED (Universal Forensic Extraction Device) software packages by Cellebrite is one of the most effective and leading forensic tools on the market today. This tool is widely used by law enforcement agencies and leading forensic expert companies around the world.

The advantages of the UFED Cellebrite software package are as follows: it has a list of all supported phone models; it can bypass locked phones and penetrate devices to gain access. If law enforcement agencies don't have passwords or codes to unlock mobile devices, a tool like UFED Cellebrite comes in handy to gain access to the device and get important information. The UFED Cellebrite software package has access to all types of USB connectors for the phone. The device can save the extracted data to USB for viewing on a regular computer. Thus, information extraction is possible using field mobile forensics and information can be extracted from the device on the spot, rather than carrying the mobile device to an expert laboratory [15].

The Oxygen Forensic Detective software package is a whole set of forensic tools that contains various types of forensic tools. When you first download the software, it automatically installs certain drivers so that you can investigate the mobile device from the moment you turn it on for the first time.

A key advantage of the Oxygen Forensic suite is its robust driver support for a broad spectrum of mobile devices. That is, it allows analyzing offline and does not require access to the Internet to download additional drivers. This makes it convenient for forensic experts who often need to work offline or outside a specialized laboratory.

The mobile device is connected to the computer via a USB cable. The installed Oxygen Forensics software package automatically detects and identifies the mobile device and connects it to the computer. After the user confirms the connection, the program starts extracting all the data from the mobile device. Oxygen Forensics also has an option to gain root access to the mobile device to bypass the locked screen. In the case of our study, this option was not used due to the risk of damage to the mobile device when trying to gain root access. That is, when working with the program under study, it is necessary to take this risk into account.

When a mobile device is connected to a computer via USB, the program automatically detects it and prompts the user to delete the data. Upon user consent, the software starts processing and extracting all the data. This process takes some time, because if there is a lot of data, it examines it in detail. he program initially makes a backup of the mobile device. Contacts, text messages, and various app data will be extracted in separate instances. As soon as the software tool completes the extraction process, it will display a section with detailed information about the mobile device, such as IMEI number, root access, device type and software revision number. All of this information is important because it can be used to further search for additional information about the device and its owner [15].

A comparative analysis of Oxygen Forensic and UFED (Universal Forensic Extraction Device) reveals both are powerful tools for mobile forensics, but they have their differences and advantages, namely:

1) Functionality and device support:

- Oxygen Forensic is a product that has extensive capabilities for analyzing various types of mobile devices, including smartphones, tablets, and even storage devices; it provides access to various types of data, including messages, photos, videos, call history, contacts, and much more.
- UFED is a product developed by Cellebrite that also supports a wide range of mobile devices and can extract a variety of data types, but has the advantage of high speed and efficiency in extracting data from different devices.

2) Interface and user experience:

- Oxygen Forensic — has an intuitive and user-friendly interface that allows quickly organizing and analyzing large amounts of data;
- UFED — the interface is also known for its simplicity and ease of use, but provides quick

access to the main functions and data analysis capabilities.

3) Analysis capabilities:

- Oxygen Forensic — provides a wider range of analytical tools and data extraction capabilities, including collecting information from social networks, GPS coordinates, apps, and more.
- UFED — known for its high efficiency in extracting basic types of data such as messages, contacts, and photos. It is commonly used to quickly get basic information from mobile devices.

4) Cost. Oxygen Forensic is a more expensive software product compared to UFED. Therefore, the choice of product depends on budget constraints and user needs.

5) Data format support.

- Oxygen Forensic — supports most data formats, which allows analyzing information from various sources, such as iCloud backups, Android backup files, Samsung backup archives, etc.
- UFED — supports many data formats, including standard backup files and specialized formats developed by various device manufacturers.

6) Update Support.

- Oxygen Forensic receives periodic updates that add new features and improve compatibility with the latest versions of mobile device operating systems.
- UFED is also updated regularly to ensure support for new devices and data formats.

7) Limitations:

- Oxygen Forensic works exclusively on the Windows platform.
- UFED operates on specialized equipment that may be more expensive and complicated for users looking for a simple solution for mobile device data analysis.

8) In Ukraine, law enforcement agencies and forensic experts use the UFED software package in 70% of cases and Oxygen Forensic in 30% of cases during criminal investigations and forensic examinations.

In the current conditions, one of the most important areas of development of the science of digital forensics and law enforcement is the formation and improvement of the field of technical and forensic research of digital data (evidence). The continuous development of scientific and technological progress, computerization of almost all spheres of production and human activity have led to the use of the latest advances in digital technologies for criminal purposes.

The article presents the characteristics, practical application process, and capabilities of each software complex, UFED (Universal Forensic Extraction Device) Cellebrite and Oxygen Forensic Detective. Also, based on the practical application results, their operation's advantages and disadvantages in extracting evidentiary information are substantiated.

Thus, based on the analysis of research and our practical application of the software package, we concluded that UFED (Universal Forensic Extraction Device) Cellebrite and Oxygen Forensic Detective are the most effective software packages for working with mobile phones, tablet computers, and storage devices.

Therefore, modern software packages for digital forensics are a powerful tool in the fight against crime, and their implementation contributes to increased security in society.

REFERENCES

1. DIGITAL 2024: GLOBAL OVERVIEW REPORT. URL: https://datareportal.com/reports/digital-2024-global-overview-report (Last accessed: 10.06.2024).
2. Matiushkova, T. P. (2021). Electronic (digital) information: current state and prospects for the evelopment of Forensic Science. *Actual Issues of Criminal Procedure and Forensic Science: International Scientific-Practical Conference (29 October, 2021, Kharkiv),* 248–250. Kharkiv
3. Meah, J. (2022). Digital Forensics: The Ultimate Guide. *Techopedia*. URL: https://www.techopedia.com/digital-forensics-the-ultimate-guide/2/34721 (Last accessed: 24.06.2024).

4. Lushchyk, I. V., Tiapkin, A. S. (2023). Problematic issues of defining digital forensics. *Theory and Practice of Jurisprudence*, 1(23), 135—160. URL: https://www.ceeol.com/search/article-detail?id=1148071 (Last accessed: 24.06.2024).
5. Mohanakrishnan, R. (2022). What is Digital Forensics? Meaning, Importance, and Types. *Spiceworks.* URL: https://www.spiceworks.com/it-security/cyberrisk-management/articles/what-is-digital-forensics/ (Last accessed: 24.03.2023).
6. Sheetz, M. (2007). *Computer Forensics. An Essential Guide for Accountants, Lawyers, and Managers.* Wiley.
7. Reedy, P. (2020). Interpol review of digital evidence 2016–2019. *Forensic Science International: Synergy*, 2, 489—520. https://doi.org/10.1016/j.fsisyn.2020.01.015
8. Kolodina, A. S., Fedorova, T. S. (2022). Digital forensics: problems of theory and practice. *Kyiv Law Journal*, 1, 176—180. https://doi.org/10.32782/klj/2022.1.27.
9. Stepaniuk, R. L., Perlin, S. I. (2022). Digital forensics and the improvement of the forensic technology system in Ukraine. *Bulletin of the Luhansk State University of Internal Affairs named after E.O. Didorenko (Ukraine)*, 3(99), 283—294. https://doi.org/10.33766/2524-0323.99.283-294
10. Venkateswara, V. Rao., Chakravarthy, A. S. N. (2016). Forensic Analysis of android mobile devices. *A.S.N Chakravarthy International Conference on Recent Advances and Innovations in Engineering (23—25 Dec 2016, Jaipur, India),* 1—6. India. https://doi.org/10.1109/ICRAIE.2016.7939540.
11. Umar, R., Riadi, I., Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *Int. J. Adv. Sci. Eng. Inf. Technol. (Indonesia),* 8(3), 949—955. https://doi.org/10.18517/ijaseit.8.3.3591
12. Osho, O., Ohida, S. O. (2016). Comparative evaluation of mobile forensic tools. *IJ Inf. Technol. Comput. Sci.*, 1, 74—83. https://doi.org/10.5815/ijitcs.2016.01.09
13. Kolesnyk, V. H., Stepaniuk, R. L. (2023). Forensic computer-technical examination: state and development prospects. *Bulletin of the Luhansk State University of Internal Affairs named after E.O. Didorenko (Ukraine),* 2, 289—305. https://doi.org/10.33766/2524-0323.102.289-305
14. Imei.info. URL: https://www.imei.info/ (Last accessed: 10.06.2024).
15. Taheem, H. (2015). Forensic Analysis on Android Mobile Devices What types of forensic data resides on Android mobile devices? British Columbia Institute of Technology Forensic Investigation. *Computer Crime Graduation* URL: https://www.stealthbay.com/wpcontent/uploads/2016/09/Harry_Taheem_Mobile_Forensics_Paper.pdf (Last accessed: 10.06.2024).
16. Criminal Procedure Code of Ukraine: Law of Ukraine dated April 13, 2012, No. 4651-VI / Bulletin of the Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n2921 (Last accessed: 10.06.2024).

Received 15.08.2024
Revised 18.03.2025
Accepted 11.04.2025

О.І. Агаркова [1] (https://orcid.org/0000-0002-6236-4198),
Л.А. Коростельова [2] (https://orcid.org/0000-0002-4782-1354),
В.Е. Краснопольський [3] (https://orcid.org/0000-0002-1413-2747)

[1] Слідче управління Головного управління
Національної поліції в Харківській області,
вул. Весніна, 14, Харків, 61023, Україна,
+380 57 730 8907, kh_su@hk.police.gov.ua
[2] Міністерство внутрішніх справ України,
вул. Академіка Богомольця, 10, Київ, 01032, Україна,
+380 44 256 0072, pgmia@mvs.gov.ua
[3] Дніпровський державний університет внутрішніх справ,
просп. Науки, 26, Дніпро, 49005, Україна,
+380 56 756 4545, info@dduvs.edu.ua

ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ПРОГРАМНИХ КОМПЛЕКСІВ У ЦИФРОВІЙ КРИМІНАЛІСТИЦІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ЗЛОЧИННОСТІ В УКРАЇНІ

Вступ. Цифрова криміналістика, що базується на використанні спеціалізованих програмних комплексів, дозволяє значно підвищити ефективність розслідування злочинів. Мобільні пристрої стали невід'ємною частиною життя як звичайного громадянина, так і правопорушника, що спричиняє нові виклики для правоохоронних органів.

Проблематика. Зростання кількості кримінальних правопорушень, пов'язаних з використанням мобільних пристроїв, вимагає застосування спеціалізованих інструментів для вилучення та аналізу великих обсягів даних, які зберігаються на таких пристроях, і надалі набувають статусу доказу у кримінальному провадженні.

Мета. Розроблення практичних рекомендацій на базі аналізу практичного використання програмних комплексів, узагальнення дослідження вилучених цифрових даних (доказів), спрямованих на використання інноваційних програмних комплексів у цифровій криміналістиці для забезпечення протидії злочинності в Україні.

Матеріали й методи. Використано програмні комплекси *UFED, Oxygen Forensic Detective, XRY, EnCase Mobile Investigator*. Проведено порівняльний аналіз можливостей цих інструментів на основі даних з реальних кримінальних проваджень. Опитано експертів у галузі цифрової криміналістики для отримання додаткових даних щодо практичного застосування програмних комплексів.

Результати. Виокремлено переваги для проведення мобільної судової експертизи кожного програмного комплексу. Визначено, що правоохоронними органами переважно використовується програмний комплекс *UFED* (*Universal Forensic Extraction Device*). Інструменти дозволяють значно скоротити час на збір та аналіз даних, підвищити точність і надійність отриманих доказів, збільшити відсоток розкриття правопорушень.

Висновки. Впровадження інноваційних технологій у роботу правоохоронних органів сприяє ефективному досудовому розслідуванню правопорушень, пов'язаних з використанням мобільних пристроїв. Рекомендації, розроблені у ході дослідження, можуть бути корисними у практичній діяльності правоохоронців.

Ключові слова: цифрова криміналістика, цифрові докази, програмні комплекси, *UFED* (*Universal Forensic Extraction Device*), *Oxygen Forensic Detective*, злочинність.