DOI: https://doi.org/10.15276/ict.01.2024.35
УДК 004.4

Логічні методи криміналістичної експертизи приладів з операційною системою Android

Ісаченко Ольга Володимирівна
Магістр каф. Інфокомунікаційної інженерії імені В.В. Поповського
E-mail: olha.isachenko@nure.ua
Харківський національний університет радіоелектроніки, пр. Науки, 14 . Харків, 61166, Україна

АНОТАЦІЯ

Мобільні пристрої зараз настільки розповсюджені, що зробили революцію в тому, як ми виконуємо більшу частину нашої діяльності. У результаті мобільний пристрій тепер є величезним сховищем конфіденційної та особистої інформації про свого власника.

Це, у свою чергу, призвело до розвитку криміналістики мобільних пристроїв, яка зосереджена на відновленні та дослідженні мобільних даних. Мета кріміналістичного процесу — отримати та відновити будь-яку інформацію з мобільного пристрою без зміни даних на пристрої. З роками цифрова криміналістика розширилася разом із швидким зростанням мобільних пристроїв. Існують різні галузі цифрової криміналістики залежно від типу цифрового пристрою, наприклад комп'ютерна криміналістика, мережева криміналістика, мобільна криміналістика тощо.

Дані, отримані з телефонів, стають безцінним джерелом доказів для розслідувань у кримінальних, цивільних справах. Рідко можна провести цифрове криміналістичне дослідження без використання телефону.

Сторонні програми є невід'ємною частиною мобільного пристрою розслідування. Для цього повинно розуміти, де на пристрої зберігаються дані програми, які дані програми зберігаються для цієї платформи та який інструмент найкраще допомагає виявити докази. Хоча деякі комерційні інструменти, такі як Magnet IEF, відомі підтримкою синтаксичного аналізу додатків, жоден інструмент не є ідеальним, і інструментам практично неможливо встигати за частими оновленнями, які випускаються для кожної програми. Найчастіше доступні комерційні інструменти аналізують найпопулярніші програми на ринку. Наприклад, коли Facebook придбав WhatsApp, Cellebrite, IEF і Oxygen Forensics почали підтримувати цю програму. Саме в цьому всі програми відрізняються.

Ключові слова: мобільна криміналістика; логічні методи; аналіз мобільних даних; криміналістичне програмне забезпечення; безпека мобільних даних

Актуальність. Криміналістика мобільних пристроїв, в силу різноманітності їх операційних систем та обладнання, потребує спеціалізованого, ніж для комп'ютерної криміналістики програмного забезпечення, яке б дозволяло вилучати та ефективно аналізувати дані з мобільних пристроїв, включаючи артефакти з найпоширеніших додатків.

Мета дослідження: проаналізувати функціональні можливості найвідомішого комерційного програмного забезпечення у сфері криміналістики мобільних пристроїв на основі операційної системі Android.

Криміналістичні методи на пристроях з операційною системою Android часто поділяють на логічні або фізичні. Логічний метод витягує дані і зазвичай досягається шляхом доступу до файлової системи. Виділення даних просто означає, що дані не видаляються та доступні у файловій системі.

Фізичні методи, з іншого боку, спрямовані безпосередньо на фізичний носій даних і не покладаються на саму файлову систему для доступу до даних. У цього підходу є переваги; найбільш важливим є те, що фізичні методи надають доступ до значної кількості видалених даних [2].

Оскільки фізичні криміналістичні методи забезпечують прямий доступ до носія даних, можна відновити як виділені, так і нерозподілені (видалені або застарілі) дані. Фізичні методи також можуть надати набагато більше даних. Однак їх складніше успішно виконати, і для їх аналізу потрібно значно більше зусиль.

Роздивимось логічні методи. Логічні методи часто є першим этапом експертизи, яку проводить аналітик, оскільки їх не тільки легше виконати, але вони часто надають достатньо даних для справи.

Логічні методи також мають перевагу так як працюють з набагато більшою кількістю сценаріїв, оскільки єдиною вимогою є ввімкнення налагодження USB. Іншими словами, логічні методи криміналістики Android не потребують кореневого доступу.

До логічних методів можно віднести роботу з утілітою adb. adb – це інструмент командного рядка, який допомагає спілкуватися з пристроєм для отримання інформації. Використовуючи adb, можно витягувати дані з усіх файлів на пристрої (до яких є доступ).

Як правило, дані на пристрої можуть зберігатися на RAM, у внутрішній пам'яті, зовнішній пам'яті, хмарах.

Щоб отримати доступ до пристрою Android через adb, необхідно ввімкнути опцію налагодження USB.

До логічного методу відноситься створення бекапу даних з пристрою. Його можно зробити за допомогою adb утіліти або вручну, користуючись інтерфейсом телефону.

Розглянемо комерційне програмне забезпечення для криміналістичної експертизи мобільних пристроїв на основі Android ОС:

- Cellebrite UFED.
- MOBILedit.
- Micro Systemation XRY.
- Oxygen Forensics.

1) Cellebrite UFED (Universal Forensic Extraction Device) – це найсучасніший інструмент, який дає доступ до найширшого спектру мобільних пристроїв та дозволяє отримувати доступ до критично важливих цифрових доказів з телефонів, дронів, SIM-карт, SD-карт, пристроїв GPS тощо [1].

Серія продуктів ізраїльської компанії Cellebrite використовується для вилучення та аналізу даних із мобільних пристроїв правоохоронними органами [2]. Останніми роками ізраїльська фірма викликала багато критики з боку активістів захисту конфіденційності даних, які стверджують, що її діяльність є неетичною. Інші атакували компанію за те, що вона не розкрила активні вразливості, які вона використовує для злому пристроїв [3].

Cellebrite UFED пропонує підтримку різних операційних систем, включаючи iOS, Android, BlackBerry та Windows Phone. За допомогою передових методів вилучення UFED може отримувати різні типи даних, наприклад журнали викликів, повідомлення, контакти, мультимедійні файли, дані програм тощо (Рис. 1).

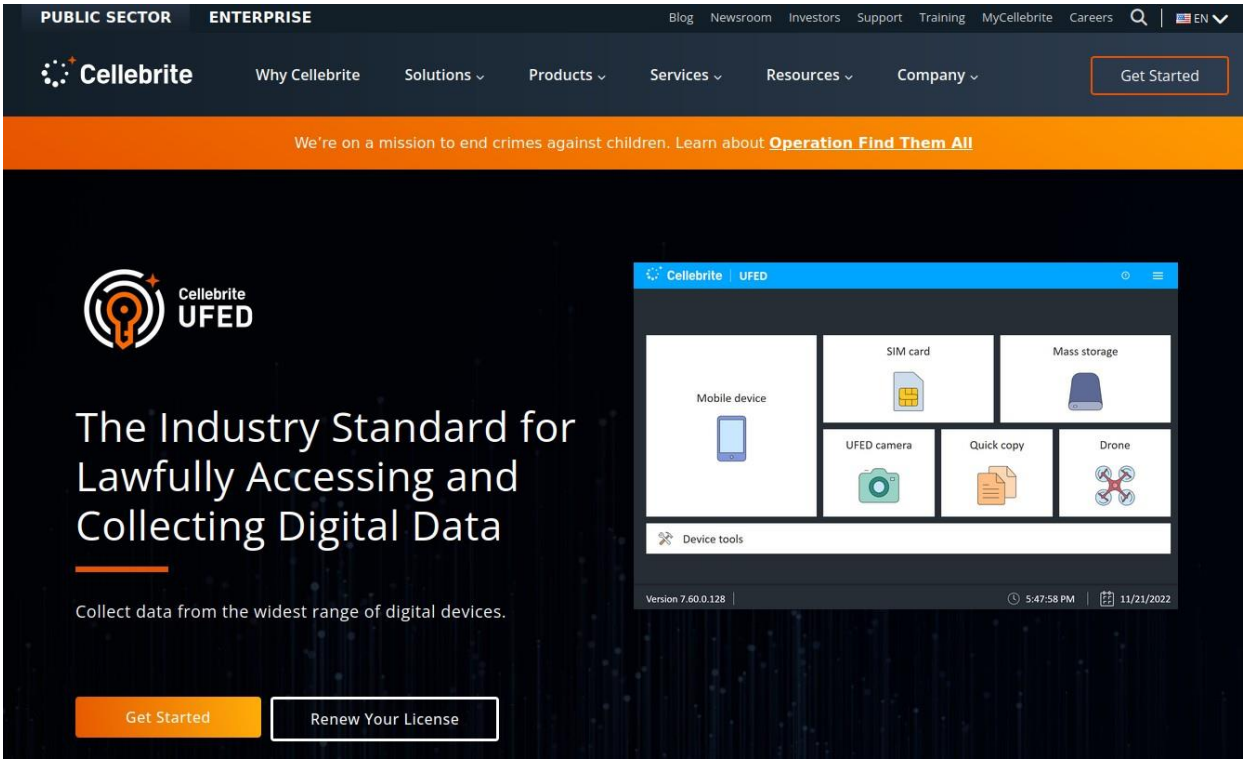

Рис. 1. **Вебсайт Cellebrite**

Cellebrite UFED пропонує два основні методи вилучення: фізичний і логічний. Фізичне вилучення передбачає створення побітової копії пам'яті пристрою, що забезпечує повне й точне представлення даних. З іншого боку, логічне вилучення зосереджується на вилученні вибраних категорій даних без доступу до всього сховища пристрою. Обидва методи пропонують унікальні переваги та пристосовані до конкретних потреб розслідування.

Після вилучення даних за допомогою Cellebrite UFED їх можна додатково проаналізувати за допомогою вбудованих можливостей аналізу інструменту або експортувати в інше програмне забезпечення для криміналістичної експертизи для поглибленого дослідження. Cellebrite UFED надає зручний інтерфейс, який дозволяє слідчим інтуїтивно досліджувати витягнуті дані. Він дає змогу здійснювати пошук, фільтрацію та сортування, а також створювати докладні звіти.

Cellebrite UFED підтримує розширені методи дешифрування та декодування для доступу до зашифрованих даних і виявлення прихованої інформації. Він може працювати з різними методами шифрування, включаючи шифрування на рівні пристрою, шифрування для конкретної програми та зашифровані бази даних. UFED використовує потужні алгоритми та бази даних для декодування паролів, відновлення видалених даних та обходу заходів безпеки.

Physical Analyzer надає розширені можливості аналізу даних, дозволяючи дослідникам візуалізувати зв'язки, часові рамки та шаблони спілкування. Він пропонує розширені функції, такі як вирізання даних, засоби перегляду SQLite і Plist, аналіз карт і інтегровані інструменти аналітики для ефективного аналізу видобутих даних.

Інтеграція з іншими криміналістичними інструментами дозволяює поєднувати переваги різних рішень для більш всебічного аналізу. Можно експортувати витягнуті дані до Magnet AXIOM, EnCase та Oxygen Forensic Detective, що забезпечує спільну роботу між інструментами та підвищує ефективність.

2) MOBILedit Forensic [4] – це цифровий криміналістичний продукт від Compelson Labs, який шукає, перевіряє та звітує про дані мобільних пристроїв GSM/CDMA/PCS. MOBILedit підключається до мобільних телефонів через інфрачервоний (ІЧ) порт, Bluetooth, Wi-Fi або кабельний інтерфейс. Після встановлення з'єднання модель телефону ідентифікується за виробником, номером моделі та серійним номером (IMEI) і відповідним зображенням телефону [5].

MOBILedit Forensic має вбудований обхід безпеки для багатьох моделей телефонів, що дозволяє отримувати фізичне зображення, навіть якщо телефон захищено паролем або шаблоном. Запроваджено новий підхід до обходу безпеки за допомогою технології Live updates – нові моделі телефонів можна додавати навіть без перевстановлення MOBILedit, як і оновлення антивірусного ПЗ (Рис. 2).

До логічного вилучення також надано збір фізичних даних Android, що дозволяє видобувати фізичні зображення досліджуваних телефонів і мати точні двійкові клони. Фізичний аналіз дозволяє відкривати файли зображень, створені цим процесом, або отримані за допомогою JTAG, chip-off чи інших інструментів для відновлення видалених файлів, а також усіх інших видалених даних.

Для аналізу програм використовуються адаптивні та глибокі методи, щоб гарантувати отримання максимум даних, доступних для кожної програми, особливо відновлення видалених даних. Дані аналізуються на предмет їхнього значення [5], тож можно бачити їх на часовій шкалі як нотатку, фотографію, відео чи потік повідомлень незалежно від того, яка програма використовувалася для їх надсилання.

Оновлення в реальному часі – це унікальна функція та сильна сторона MOBILedit Forensic, яка забезпечує негайне оновлення аналізу програм, обходу безпеки та інших функцій у реальному часі та так часто, як це необхідно.

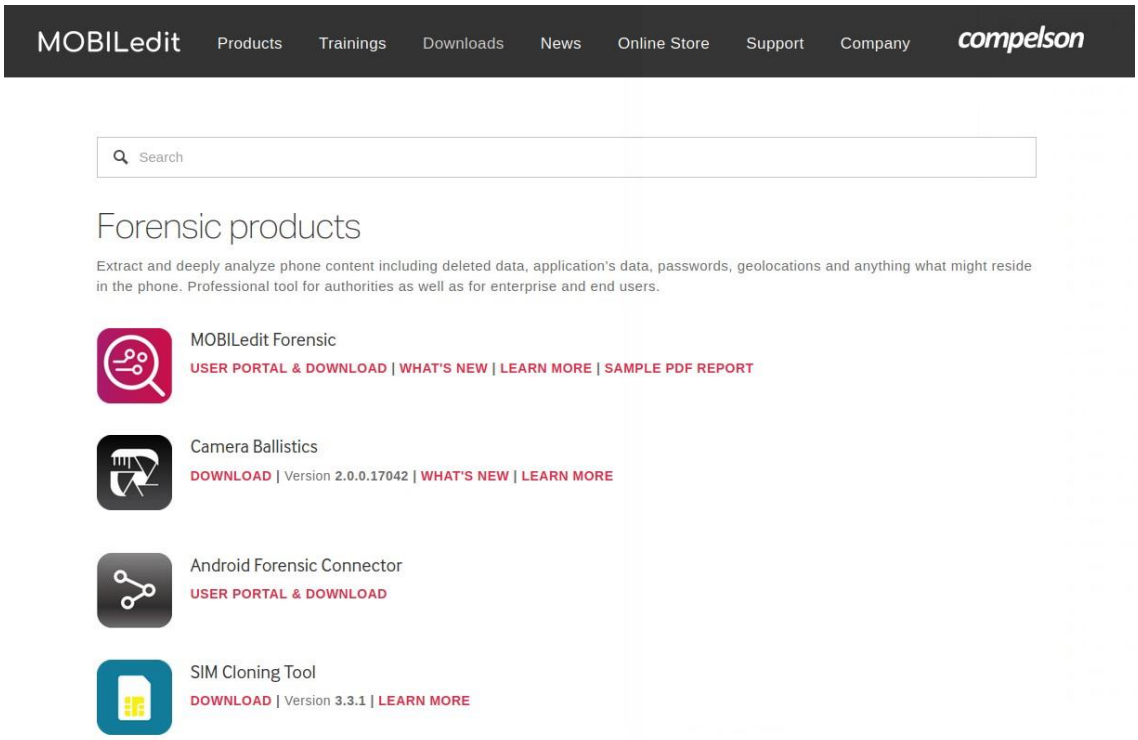

Рис. 2. **Спектр продуктів MOBILedit**

Крім отримання вмісту телефону, видобування з хмари є необхідністю для отримання всіх можливих даних. MOBILedit Cloud Forensic підтримує найпопулярніші хмарні сервіси, такі як Booking, Microsoft Teams, Dropbox, Box, Microsoft OneDrive, Google Drive, Facebook, Instagram, LinkedIn, Twitter, Facebook Messenger, Slack та багато інших. Ця потужна функція доступна як окремий продукт або може бути інтегрована в MOBILedit Forensic Pro.

3) Micro Systemation XRY – це інструмент криміналістичної експертизи мобільних пристроїв, розроблений Micro Systemation, який надає інтуїтивно зрозумілий і зручний інтерфейс для аналізу широкого діапазону мобільних телефонів [7] та включає програмне та апаратне забезпечення для логічного та фізичного аналізу мобільних пристроїв (Рис. 3).

Можливо, найвідомішим і найнадійнішим пакетом є XRY Logical [6]. Програмне забезпечення аналізує та отримує поточні (живі) дані з пристрою.

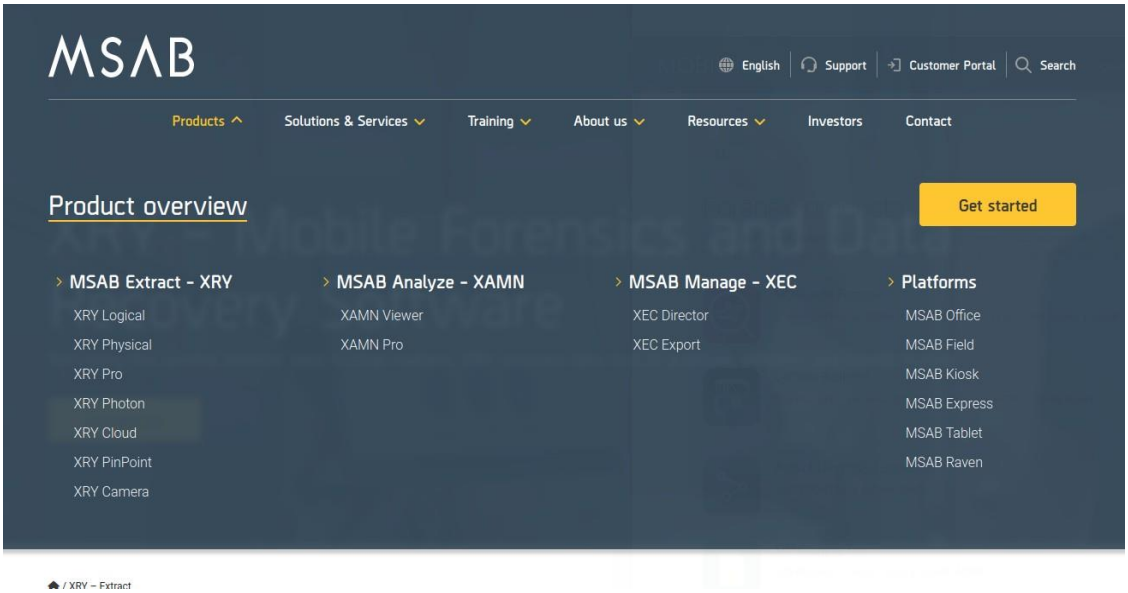

Рис. 3. **Асортимент продуктів Micro Systemation**

Один з нових пакетів - XRY Pinpoint – це сучасне компактне обладнання та потужне програмне забезпечення, яке дозволяє користувачам витягувати та декодувати дані з нестандартних мобільних пристроїв. PinPoint може автоматично визначати конфігурацію контактів, щоб спілкуватися з мобільним пристроєм.

4) Oxygen Forensics відомий насамперед своїм простим у використанні інтерфейсом. Початкове підключення до мобільного пристрою здійснюється за допомогою майстра, що робить його досить простим у використанні (Рис. 4).

Oxygen Forensic Detective – це високофункціональний програмний інструмент [8], який використовується для цифрових криміналістичних досліджень мобільних пристроїв і хмарних сховищ.

Він може використовуватися для:

- Отримання даних з пристроїв (Android, BB, iOS, WP тощо).
- Імпорту резервних копій і зображень (iTunes, Android, JTAG, Chip-Off).
- Аналізу даних з програм.
- Відновлення видалених даних.
- Аналізу даних (соціальний графік, хронологія, ключові докази).
- Пошуку даних за критеріями, включаючи ключові слова.
- Відновлення паролів до зашифрованих резервних копій і зображень.
- Обхіду блокування екрана на популярних пристроях з ОС Android.

Висновки. За допомогою наведеного комерційного програмного забезпечення можна провести криміналістичне дослідження пристрою з операційною системою Android. Якщо пристрій захищено паролем, щоб отримати дані необхідно обійти захист. Хоча існує різні методи обходу коду доступу, неможливо досягти цього за будь-яких обставин. Коли пристрій стає доступним, можно вибрати між логічним збором, який зосереджується в основному на невидалених даних, або більш ретельним, але технічно складним фізичним збором. Тоді як фізичне отримання дасть більше даних.

Більшість комерційного програмного забезпечення дозволяє вилучити та проаналізувати основні дані з телефону, такі як контакти, журнали викликів, GPS координати, фото/відео, історію пошуку, загальні файли.

Комерційне програмне забезпечення як правило надає більш функціоналу та можливостей що до вилучення та аналізу даних, ніж програмне забезпечення з відкритим кодом.

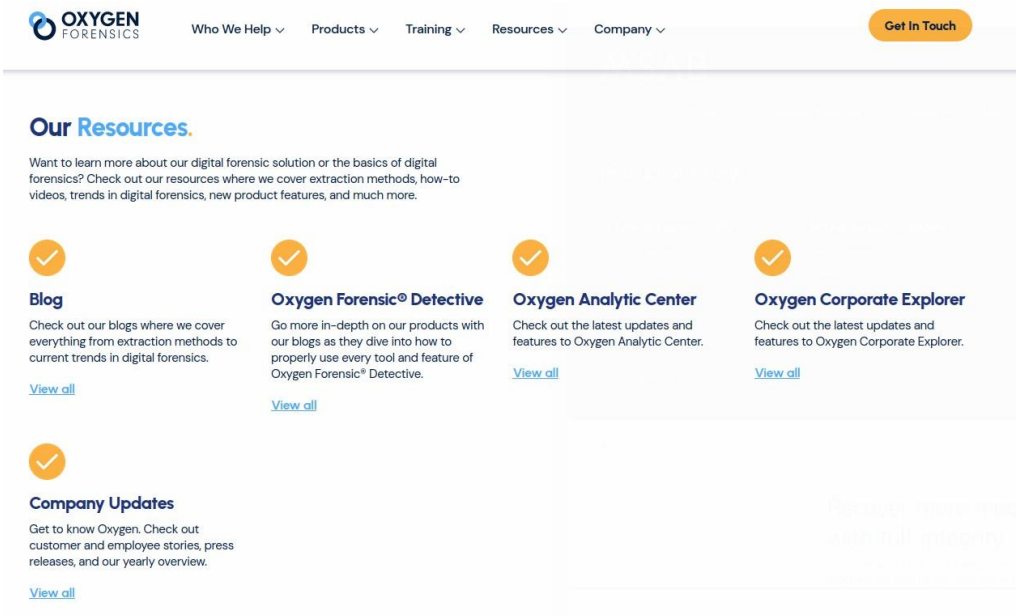

Рис. 4. **Продуктова лінійка Oxygen Forensic**

СПИСОК ЛІТЕРАТУРИ

1. «Інформація з вебсайту “Cellebrite”». – Available from: https://cellebrite.com/en/ufed/ (дата звернення: 02.09.2023)

2. Zhao Y., Zhou T., Chen Z. & Wu J. “Improving deep CNN networks with long temporal context for text independent speaker verification”. *IEEE International Conference on Acoustics, Speech and Signal Processing*. 2020. p. 6834–6838. DOI: https://doi.org/10.1109/ICASSP40776.2020.9053767.

3. «Інформація з вебсайту Wikipedia. “Cellebrite UFED”». – Доступно з: https://en.wikipedia.org/wiki/Cellebrite_UFED. – (Дата звернення: 24.08.2024).

4. Khalili, J. “Cellebrite: The mysterious phone-cracking company that insists it has nothing to hide”. – Available from: https://www.techradar.com/news/cellebrite-the-mysterious-phone-hacking-company-that-insists-it-has-nothing-to-hide 2021. – (Дата звернення: 24.08.2024).

5. Leoshchenko S. D., Oliynyk A. O. , Subbotin S. O., Hoffman E. O., Kornienko O. V. “Method of structural adjustment of neural network models to ensure interpretability”. *Radio electronics, Computer Science, Control*. 2021; 3: 86–96. DOI: https://doi.org/10.15588/1607-3274-2021-3-8.

6. «Інформація з вебсайту “Compelson”». – Доступно з: https://www.mobiledit.com/. – (Дата звернення: 24.08.2024).

7. «Інформація з вебсайту Wikipedia “MOBILedit”».– Доступно з: https://en.wikipedia.org/wiki/MOBILedit. – (Дата звернення: 22.08.2024).

8. «Інформація з вебсайту “MSAB”».– Доступно з: https://www.msab.com/product/xry-extract/. – (Дата звернення: 24.08.2024).

9. «Інформація з вебсайту “XRY Logical”». – Доступно з: https://www.msab.com/wp-content/uploads/2022/06/XRY_Logical_EN-2.pdf.

10. «Інформація з вебсайту “Oxygen Forensics”». – Доступно з: https://oxygenforensics.com/en/. – (Дата звернення: 22.08.2024).

11. Komleva N. O., Liubchenko V. V. & Zinovatnaya S. L. “Methodology of information monitoringand diagnostics of objects represented by quantitative estimates based on cluster analysis”. *Applied Aspects of Information Technology*. *Publ. Nauka i Tekhnika*. Odesa. Ukraine: 2020; 3 (1): 375–392. DOI: https://doi.org/10.15276/aait.01.2020.1.

DOI: https://doi.org/10.15276/ict.01.2024.35
UDC 004.4

Logical methods of forensic expertise of Android devices

Olha V. Isachenko
Master, faculty Infocommunication Engineering named after V.V. Popovsky
E-mail: olha.isachenko@nure.ua
Kharkiv National University of Radio Electronics, 14, Nauka Ave. Kharkiv, 61166, Ukraine

ABSTRACT

Mobile devices are now so ubiquitous that they have revolutionized the way we do most of our activities. As a result, the mobile device is now a huge repository of confidential and personal information about its owner.

This has led to the development of mobile forensics, which focuses on the recovery and investigation of mobile data. The purpose of the diagnostic process is to retrieve and recover any information from a mobile device without changing the data on the device. Over the years, digital forensics has expanded with the rapid growth of mobile devices. There are different branches of digital forensics depending on the type of digital device, such as computer forensics, network forensics, mobile forensics, etc.

Data obtained from telephones becomes an invaluable source of evidence for investigations in criminal and civil cases. It's rare to conduct digital forensics without using a phone.

Third-party applications are an integral part of the investigation mobile device. This requires understanding where app data is stored on the device, what app data is stored for that platform, and which tool best helps uncover the evidence. Although some commercial tools, such as Magnet IEF, are known for supporting application parsing, no tool is perfect, and it is nearly impossible for tools to keep up with the frequent updates that are released for each application. The most commonly available commercial tools analyze the most popular programs on the market. For example, when Facebook acquired WhatsApp, Cellebrite, IEF, and Oxygen Forensics started supporting the app. This is where all programs differ.

Keywords: Mobile forensics; logistics methods; mobile data analysis; forensics software; mobile data security