

УДК 004.63

Бойко М.В.^{1,2}

¹ асп., кафедра комп'ютерних наук, Сумський державний університет

² старший детектив, Підрозділ детективів цифрової криміналістичної лабораторії, Національне антикорупційне бюро України

МЕТОД ЗБЕРЕЖЕННЯ ЗНИКАЮЧИХ ПОВІДОМЛЕНЬ НА ТЕЛЕФОНАХ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

Вагому роль при розслідуванні кримінальних проваджень відіграє електронна переписка, виявлена на різних мобільних пристроях фігурантів розслідування. Переважна більшість месенджерів зберігають історію повідомлень у базах даних SQLite. За певних умов видалені повідомлення можуть ще зберігатися певний час у різних частинах цих баз даних або в відповідних файлах WAL та journal. Проте стан цих сховищ повідомлень змінюється в залежності від налаштувань, зроблених розробниками

месенджерів, від активності користувача, налаштувань телефону тощо. Під час проведення цифрових досліджень відновлення видалених повідомлень є доволі складною задачею з невизначеним наперед результатом [1, 2].

Мета роботи – розробити метод, що дозволяє зберегти зникаючі повідомлення на телефонах Android та/або мінімізувати ризики їх знищення до моменту створення копії.

Під час дослідження використовувалися телефони Xiaomi Redmi Note 7 (Android 10) та Samsung A52s 5G (Android 14), на яких було встановлено такі месенджери, як: Signal (v. 7.21.5, 7.22.2), WhatsApp (v. 2.24.21.79), Telegram (v. 11.2.2, 11.2.3), Viber (v. 23.8.3.0), Zangi (v. 6.0.9). На телефонах у кожному з месенджерів створено переписку між двома співрозмовниками з використанням таймерів автовидалення повідомлень. Періоди автовидалення повідомлень обиралися рівними 1 хвилині, 1 годині або 1 добі, де це було можливо.

Після цього розглянуто питання впливу наступних маніпуляцій з налаштуваннями телефону на схоронність зникаючих повідомлень при:

- переведення телефону в режим польоту без зміни часу [3];
- переведення телефону в режим польоту зі зміною часу;
- зміна часу телефону з подальшим переведення в режим польоту;
- переведення телефону в режим польоту та примусове завершення роботи додатків без проведення інших маніпуляцій.

В останньому випадку з метою перевірки схоронності повідомлень через 24-72 години після сплину терміну автовидалення повідомлень створювалися копії повної файлової системи телефонів. При цьому телефони перебували у ввімкненому стані та могли як перезавантажуватися, так і ні.

У результаті перших трьох етапів дослідження встановлено, що зникаючі повідомлення в месенджерах Whatsapp, Viber, Telegram видаляються рівно через зазначені періоди часу незалежно від наявності/відсутності мережі та від переведення час телефону назад/вперед. Натомість знищення зникаючих повідомлень у Signal і Zangi відбувалося тільки в намічені дату та час згідно таймера телефону. Тобто переведення часу телефону назад запобігало видаленню повідомлень у месенджерах Signal і Zangi. При цьому Zangi при маніпуляціях з часом взагалі переставав видаляти повідомлення. Лише перезапуск застосунку поновлював цей процес.

У випадку з примусово закритими додатками усі зникаючі повідомлення, які повинні були видалитися, збереглися у створеній копії даних у всіх випадках. Під час цього етапу додатково зафіксовано кількість відновлених повідомлень з числа тих, що вже видалилися з чатів на момент примусового завершення роботи месенджерів. У таблиці 1 наведено кількість таких відновлених повідомлень з телефону Xiaomi. При пошуку за словами

серед баз даних месенджерів жодного іншого видаленого повідомлення не виявлено. У випадку з Whatsapp було відновлено останні повідомлення. Аналогічно під час створення інших копій іноді могли бути відновленими декілька останніх повідомлень у месенджерах Signal і Zangi. Ці результати корелюються з іншими роботами [1, 2].

Таблиця 1 – Дані щодо відновлених повідомлень

Пристрій	Назва месенджера	Отримані	Надіслані
Xiaomi Redmi Note 7 (Android 10)	Viber	4/12	3/12
	Whatsapp	7/15	5/12
	Telegram	0/15	0/20
	Telegram secret chat	0/12	0/12
	Signal	0/10	0/15
	Zangi	0/12	0/13

Отже у випадку необхідності збереження зникаючих повідомлень у месенджерах на телефонах Android можна запропонувати метод, який полягає в таких кроках:

- переведення телефону в режим польоту;
- примусове завершення роботи додатків.

Цей метод дозволяє удосконалити алгоритми дій осіб, що проводять вилучення незаблокованих телефонів Android з доступом до управління його налаштуваннями [3]. Для цього пропонується після переведення телефону в режим польоту перед виконанням інших дій примусово завершити дії месенджерів (рисунок 1). Це повинно зафіксувати стан баз даних SQLite, що містять історію електронної переписки, та запобігти видаленню/зміні даних. Переведення дати назад може застосовуватися опціонально.



Рисунок 1 – Удосконалення алгоритму дій при вилученні телефону на базі операційної системи Android.

Таким чином можна сказати таке. Маніпуляції з часом не сприяють збереженню зникаючих повідомлень у месенджерах Viber, WhatsApp,

Telegram на телефонах Android. Переведення дати назад у налаштуваннях телефонів Android при їх вилученні може бути використано в окремих випадках (наприклад, для збереження повідомлень у месенджерах Signal, Zangi). Як видно з таблиці 1, результати відновлення вже видалених зникаючих повідомлень є незадовільними в усіх випадках. Тому в загальному випадку для збереження зникаючих повідомлень та/або мінімізації ризиків їх видалення рекомендується примусово завершувати роботу месенджерів, дані з яких становлять інтерес для досудового розслідування.

Висновок. Представлений метод збереження зникаючих повідомлень дозволяє зберегти цифрові сліди кримінального правопорушення на телефонах Android. За допомогою цього методу можна вдосконалити стандартні алгоритми дій при вилученні незаблокованих телефонів Android, що дозволить запобігти видаленню зникаючих повідомлень та/або зменшити ризики їх видалення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Vasilaras, A., Dosis, D., Kotsis, M. and Rizomiliotis, P., “Retrieving Deleted Records from Telegram,” *Forensic Science International: Digital Investigation*, 2022, vol. 43. DOI: 10.1016/j.fsidi.2022.301447.

2. Heath, H., MacDermott, Á. and Akinbi, A., “Forensic Analysis of Ephemeral Messaging Applications: Disappearing Messages or Evidential Data?,” *Forensic Science International: Digital Investigation*, 2023, vol. 46. DOI: 10.1016/j.fsidi.2023.301585.

3. Interpol, “Guidelines for digital forensics first responders: Best practices for search and seizure of electronic and digital evidence”, Interpol, no. March, 2021.