УДК 004.056:343.98]:004.77

МЕТОДИКА ЦИФРОВОГО КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ МЕСЕНДЖЕРІВ

Рєзніченко Д.Ю.
Науковий керівник – доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(099) 790-70-05

This work is devoted to research in the field of digital forensics, more specifically – forensics of messengers. Three most popular today's messengers were considered, and the possible working methods of obtaining personal information of users from these messengers were investigated and described.

In addition, a list of information that could be obtained from messengers was specified. It is also important to note that all the described methods are relevant for Windows and Android operating systems. Moreover, a prerequisite for all experiments was the presence of a physical device (phone, laptop or computer) of the suspect in the hands of a digital forensic investigator.

Сьогодні месенджери стали невід'ємною частиною нашого життя. За їх допомогою можна безкоштовно та без обмежень спілкуватися з людьми із різних країн, здійснювати швидкий обмін будь-якими файлами (фото, відео, документи тощо), створювати публічні та приватні тематичні групи тощо. Усе вищезазначене є відповіддю на питання величезної популярності месенджерів.

Але така популярність часто привертає увагу не лише нових потенційних користувачів, а й зловмисників (наприклад, хакерів). Крім цього, дослідженням месенджерів часто займаються й правоохоронні органи, оскільки цими додатками нерідко користуються злочинці (наприклад, для планування терактів, обміну забороненими матеріалами тощо). В останньому випадку має місце цифрова криміналістика (пошук, отримання, дослідження та закріплення цифрових доказів).

В рамках написання кваліфікаційної роботи бакалавра було проведено дослідження механізмів цифрового криміналістичного аналізу трьох популярних месенджерів: Viber, WhatsApp та Telegram.

Особливості методики цифрового криміналістичного аналізу месенджера Viber. Цей месенджер можна вважати найбільш небезпечним з усіх вищезазначених, оскільки він зберігає всі дані (переписки, пересланні фото, відео, документи та інше) у незашифрованому вигляді на мобільному пристрої чи комп'ютері самого користувача. Щоб прочитати ці дані, необхідно лише знайти файл «viber.db» (зазвичай він зберігається у локальних файлах месенджера) та відкрити його за допомогою програми SQLiteStudio. У «viber.db» можна побачити наступну інформацію: текстові повідомлення з приватних чатів користувача; персональну інформацію контактів користувача (дата народження, номер телефону, імена тощо); перелік публічних та приватних чатів, членом яких є користувач; назви й

ідентифікатори файлів, які було переслано або отримано користувачем через Viber, а також багато іншого. Крім цього, всі фото й відео, які користувач отримав чи переслав через Viber, можна побачити в окремих папках за адресами: «Android\data\com.viber.voip\files» (для Android) і «C:\Users\”користувач”\ AppData\Roaming\ViberPC\”номер телефону”» (для Windows).

Особливості методики цифрового криміналістичного аналізу месенджера WhatsApp. Цей месенджер, як і Viber, зберігає всю інформацію користувача на його власному пристрої. Але ці дані вже є зашифрованими стійким блоковим криптографічним алгоритмом AES-256 (у режимі GCM). Для їх розшифрування з мобільного пристрою потрібно дістати спеціальний ключ, який зазвичай зберігається у «…/data/data/files/key» директорії. Доступ до цієї директорії можливий тільки за наявності на мобільному пристрої root-прав (за замовчуванням їх немає). Якщо ключ є, з WhatsApp можна дістати: тексти листувань, інформацію про голосові та відеодзвінки, технічні дані месенджера, номери телефонів та інші персональні дані контактів користувача тощо. Варто також зазначити, що всі користувацькі дані WhatsApp зберігає в окремому файлі «msgstore.db.crypt14», який можна знайти за шляхом: «…\Android\media\com.whatsapp\WhatsApp\Databases» (для Android) та «C:\Users\”користувач”\AppData\Local\Packages\ 5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState» (для Windows). Медіафайли (фото, відео тощо) месенджера можна також знайти у цих двох директоріях. Варто також додати, що WhatsApp, як і Viber, видаляє всі метадані медіафайлів (неможливо дізнатися, де було зроблено фото, на який пристрій тощо). Особливості методики цифрового криміналістичного аналізу месенджера Telegram. Telegram є найбільш захищеним месенджером, оскільки всі переписки та персональні дані він зберігає на власних серверах, а не на пристрої користувача. З Telegram можна витягнути лише медіафайли та голосові повідомлення, які зберігаються у відкритому вигляді за адресами: «…\Android\data\org.telegram.messenger \files\Telegram» (для Android) та «C:\Users\”користувач”\Downloads\ Telegram Desktop» (для Windows). Мінусом є те, що Telegram не видаляє метадані медіафайлів.

Список використаних джерел:

1. Viber для Windows и история сообщений [Електронний ресурс] // Habr. – 08.02.2016. – Режим доступу: https://habr.com/ru/articles/276777/. – Назва з титул. екрану.

2. FAQ for the Technically Inclined [Електронний ресурс] // Core.telegram. Режим доступу: https://core.telegram.org/techfaq#q-how-does-end-to-end-encryption-work-in-mtproto. – Назва з титул. екрану.

3. How to decrypt whatsapp crypt14 files [Електронний ресурс] // YouTube. – 12.03.2022. – Режим доступу: https://www.youtube.com/watch?v= TBL72KqemGs&list=LL&index=1&t. – Назва з титул. екрану.