Вилучення файлів із пам'яті мобільного телефону Apple Iphone, збережених у cache-пам'яті програмного забезпечення «Telegram»

Іван Старенький

судовий експерт, Одеський НДІСЕ Мін'юсту України, м. Одеса, Україна,
ORCID: http://orcid.org/0009-0004-2271-8512, e-mail: ivan_starenkii@ukr.net

Олександра Донченко

старша судова експертка, Одеський НДІСЕ Мін'юсту України, м. Одеса, Україна,
ORCID: http://orcid.org/0009-0005-3907-2372, e-mail: donchenko2707@gmail.com

Розглянуто рекомендації щодо дій експерта під час проведення комп'ютерно-технічної експертизи апарату стільникового зв'язку марки «Apple Iphone».

Ключові слова: *програмне забезпечення; операційна система; апарат стільникового зв'язку; Apple Iphone.*

Extracting Files from the Cache Memory of Telegram Software on an Apple iPhone

Ivan Starenkyi, Oleksandra Donchenko

The paper provides recommendations on the forensic expert's actions during forensic computer examination of the brand 'Apple iPhone' cell phone.

Keywords: *software; operating system; cell phone; Apple iPhone.*

Під час проведення комп'ютерно-технічних експертиз із дослідження апаратів стільникового зв'язку (далі — *АСЗ*) поміж поставлених перед експертом завдань у переважній більшості випадків необхідно визначити перелік установленого в пам'яті АСЗ програмного забезпечення (далі — *ПЗ*) з обміну миттєвими повідомленнями з подальшим отриманням історій листування користувача АСЗ із контактами в середовищі виявлених програмних продуктів (далі — *ПП*).

З метою отримання історій листування за допомогою ПЗ «WhatsApp», «Viber», «Telegram» та ін., експертом використовується один або кілька спеціалізованих криміналістичних програмних продуктів (далі — *СКПП*), таких як «Cellebrite UFED (Universal Forensic Extraction Device)» [1], «Oxygen Forensic Detective» [2], «Magnet AXIOM» [3], «Elcomsoft Mobile Forensic Bundle» [4].

Також окремим питанням може бути отримання файлів, що містяться в історії листування між певними контактами в середовищі ПЗ з обміну миттєвими повідомленнями (месенджер). У такому разі на результативність виконання даного завдання впливає кілька умов.

Ключовою умовою отримання будь-якого файлу, що міститься в історії листування месенджеру, є вимога, щоб відповідний файл було збережено до Cache-інформації месенджеру, тоді СКПП під час сканування інформаційного наповнення пам'яті АСЗ зможе скопіювати даний файл у свій звіт щодо результатів сканування мобільного пристрою (далі — *МП*). І саме на даному етапі виникає друга умова успішності виконання завдання в отриманні файлу з історії листування.

Історично склалося так, що переважно станом на сьогодні операційними системами (далі — *ОС*), на яких працюють МП, є «Android» та «iOS».

ОС «Android» відкрита, із відкритим вихідним кодом (на основі «Linux»), розроблена компанією «Google», дає змогу більшого

рівня кастомізації. Користувачі можуть змінювати інтерфейс, установлювати сторонні магазини застосунків (наприклад, «Amazon Appstore») або навіть завантажувати інсталяційні APK-файли безпосередньо з інтернету.

«iOS», на противагу «Android», є закритою ОС, розроблена компанією «Apple», вихідний код якої недоступний для публічного використання, з обмеженою кастомізацією, усі застосунки мають бути завантажені лише через офіційний магазин «App Store».

Тому у випадку дослідження АСЗ марки «Apple Iphone» експерт може зіштовхнутися з тим, що через політику безпеки ПЗ з обміну миттєвими повідомленнями, зокрема «Telegram» (надалі в роботі мова буде йти в розрізі ПЗ «Telegram»), саме для МП марки «Apple» Cache-інформація месенджера буде зберігатися в захищеному (зашифрованому) контейнері самого застосунку.

Це означає, що файли, такі як фото, відео, документи тощо за умови, якщо не було змінено теки зберігання таких файлів, ви можете переглянути лише в середовищі застосунку ПЗ «Telegram», а СКПП не зможе скопіювати дані файли до свого звіту.

Файли, не збережені в Cache-пам'яті застосунку ПЗ «Telegram», установленого в пам'яті АСЗ, в середовищі історії обміну файлів контактів позначені блакитною стрілочкою (рис. 1), тоді як файли, збережені в Cache-пам'яті, даної стрілки не містять.

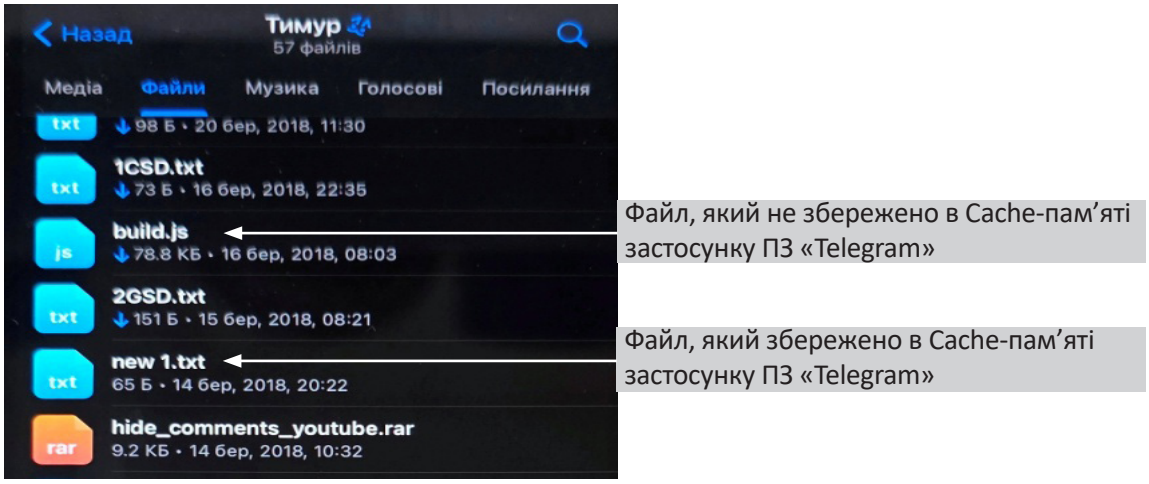

Рис. 1. Перелік файлів в історії обміну файлами ПЗ «Telegram»

У зв'язку з цим часто буває так, що у випадках дослідження АСЗ марки «Apple Iphone» інформаційний уміст деяких файлів, наприклад, текстових, фіксується експертом шляхом фотографування їх вмісту.

Але не абсолютно всі файли можуть бути переглянуті в середовищі ПЗ «Telegram» безпосередньо на АСЗ, тому авторами даної роботи пропонується метод отримання будь-якого файлу, збереженого в Cache-пам'яті застосунку ПЗ «Telegram», установленого в пам'яті АСЗ. Суть даного методу полягає в копіюванні файлу із зашифрованого контейнера ПЗ «Telegram» до незашифрованого контейнера ПЗ «Файлы», який є стандартним ПП для мобільних пристроїв марки «Apple» (див. рис. 2—8).

Рис. 2. Файл, який необхідно дослідити

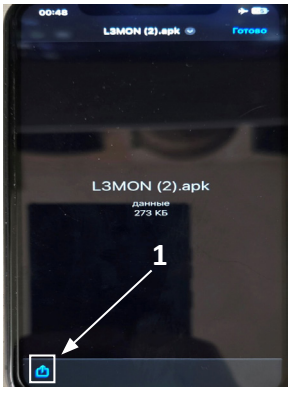

Рис. 3

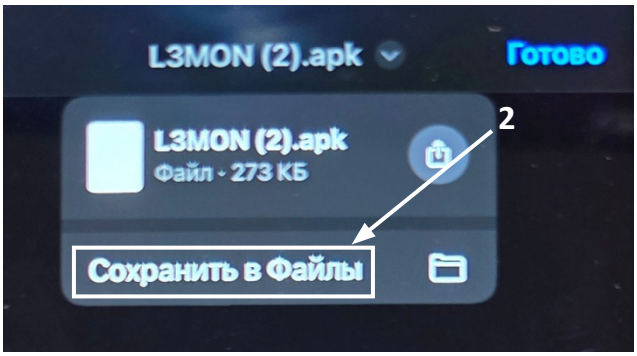

Рис. 4

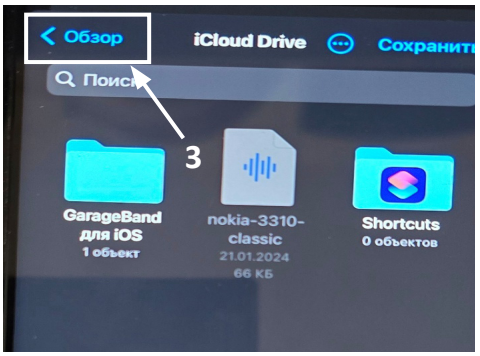

Рис. 5

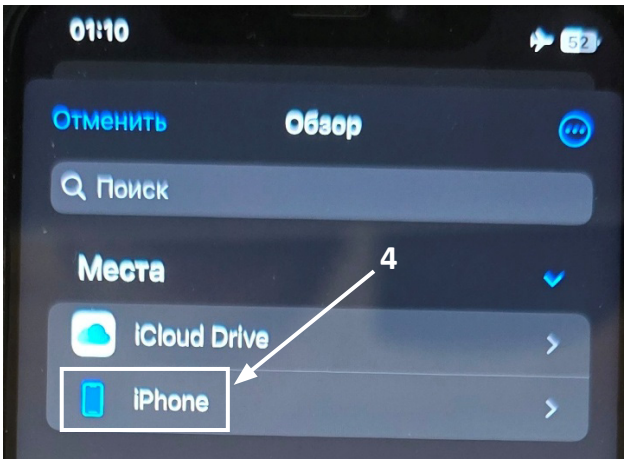

Рис. 6

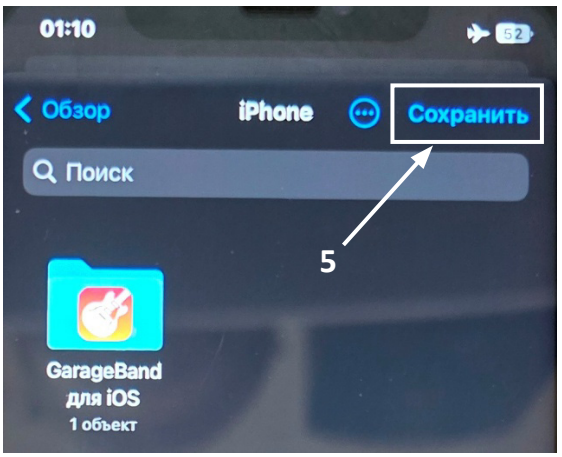

Рис. 7

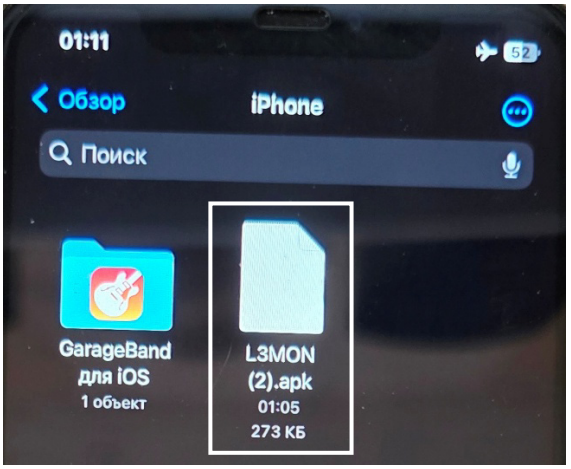

Рис. 8

Рис. 3—8. Збереження файлу «L3MON (2).apk» із Cache-інформації ПЗ «Telegram» до ПЗ «Файлы»

Необхідна умова для виконання наведених на рис. 3—8 дій — отримання від замовника дозволу на внесення змін до первинного стану АСЗ.

Отже, після виконання проілюстрованих вище дій, СКПП під час сканування пам'яті АСЗ зможе виявити та скопіювати до свого звіту необхідний файл(и). Але через те, що файл «L3MON (2).apk» (проілюстрований випадок) було скопійовано із Cache-інформації ПЗ «Telegram» до ПЗ «Файлы», його «оригінальні» часові характеристики будуть змінені, це також необхідно брати до уваги під час проведення експертизи.

Перелік джерел посилання

1. Cellebrite UFED (Universal Forensic Extraction Device). URL: https://cellebrite.com/en/ufed/ (дата звернення: 16.09.2024).
2. Oxygen Forensic Detective. URL: https://oxygenforensics.com/ (дата звернення: 16.09.2024).
3. Magnet AXIOM. URL: https://www.magnetforensics.com/ (дата звернення: 16.09.2024).
4. Elcomsoft Mobile Forensic Bundle. URL: https://www.elcomsoft.com/ (дата звернення: 16.09.2024).