МЕТОДИКА ПРОВЕДЕННЯ ЦИФРОВОЇ КРИМІНАЛІСТИЧНОЇ ЕКСПЕРТИЗИ МЕСЕНДЖЕРІВ

Рєзніченко Д.Ю., Снігуров А.В.

Харківський національний університет радіоелектроніки,
Україна

E-mail: dymytrii.rieznichenko@nure.ua,
arkadii.snihurov@nure.ua

Abstract

This work is devoted to research in the field of digital forensics, more specifically - forensics of modern messengers. This work briefly describes the internal structure of Viber, Telegram and WhatsApp messengers. Also, the methodology developed for their research is presented. In addition, this study shows examples of the use of the developed methodology for the search and research of messenger artifacts. It is worth noting that the method shown in this work is relevant only for Windows and Android operating systems.

Дослідження внутрішньої структури месенджерів

Месенджери Viber, WhatsApp та Telegram мають високий рівень популярності. За їх допомогою кожен день сотні мільйонів людей здійснюють голосові та відеодзвінки, пересилають медіафайли, відправляють один одному голосові і текстові повідомлення тощо. При проведенні розслідувань злочинів месенджери можуть дати правоохоронним органам значну кількість необхідної інформації. Питання цифрової криміналістики месенджерів досліджувалися авторами в [1,2]. В даній роботі приводяться більш детальні результати даних досліджень. Спочатку проведемо аналіз внутрішньої структури месенджерів. Почнемо з Viber та Viber Mobile.

Viber та Viber Mobile мають дуже схожу структуру. На поточний момент основною базою даних цього месенджеру є Couchbase. Couchbase є системою управління базами даних класу NoSQL (тобто доступ до даних здійснюється без використання спеціальної мови SQL). Couchbase дозволяє організувати зберігання даних як на одному вузлі, так і у формі розподіленої системи, інформація в якій розміщується поверх групи серверів. Couchbase також має вбудовані засоби для забезпечення високого рівня доступності даних, самовідновлення (у разі збою вузлів, що обслуговують сховище інформації) та побудови сегментованих сховищ, резервні копії яких зберігатимуться у різних дата-центрах. Разом з Couchbase використовується й кеш Redis, який дозволяє значно підвищити продуктивність бази даних. Загалом, Couchbase прийшла на заміну MongoDB, оскільки остання мала значні проблеми з масштабованістю та швидкістю обробки великих масивів користувацьких даних [3].

Основні файли-бази месенджера Viber мають назви «viber.db» (для Windows) та «viber_messages.db» і «viber_data.db» (для Android). Варто також зазначити, що ці файли, починаючи з 2023 року, є зашифрованими і прочитати їх може лише сам месенджер.

Захист даних у Viber та Viber Mobile організований на основі спеціальної модифікації Signal Protocol від компанії Open Whisper Systems [4]. Модифікований варіант протоколу Signal, який використовується у Viber, заснований на Double Ratchet Algorithm, що є комбінацією протоколу обміну ключами Діффі-Хеллмана та функції формування самого криптографічного ключа (у Viber ця функція заснована на Hash-based Message Authentication Code та Secure Hash Algorithm 256).

Разом з модифікованою версією Signal Protocol, у месенджері Viber застосовується й Zimmermann Real-time Transport Protocol, який використовується для шифрування трафіку голосових та відеодзвінків.

Далі проаналізуємо WhatsApp та WhatsApp Mobile. Всі складові цього месенджера (база даних, сервери, протоколи) написані мовою програмування Erlang [5]. Erlang має значний ступінь паралелізму, масштабованості, надійності та використовує модель, в якій невеликі ізольовані процеси взаємодіють

один з одним за допомогою спеціальних повідомлень. Для компіляції коду, написаного на Erlang, використовується віртуальна машина Bogdan's Erlang Abstract Machine.

Основною базою даних месенджера WhatsApp є Mnesia. Mnesia має складні об'єкти, динамічну реконфігурацію, високий рівень відмовостійкості та можливість пошуку пар «ключ-значення» у режимі реального часу. Все вищезазначене можна вважати основними перевагами бази даних «Mnesia».

Крім Mnesia, месенджер WhatsApp використовую ще й базу даних «SQLite». SQLite є автономною реляційною базою даних, яка вбудовується в додаток та існує на кінцевому пристрої користувача. Загалом, на SQLite побудований зовнішній інтерфейс месенджера WhatsApp. Основними файлами бази SQLite можна вважати «messages.db» (для Android це «messages.db.crypt*»), «axolotl.db» «contacts.db», «settings.db» та «wa.db». Деякі вищезазначені файли (наприклад, «messages.db») є зашифрованими.

Захист користувацьких даних у месенджері WhatsApp реалізований на основі Signal Protocol. Основою Signal Protocol є Double Ratchet Algorithm та протокол обміну ключами Діффі-Хеллмана, а у якості примітивів використовуються Curve-25519, Advanced Encryption Standard -256 та HMAC-SHA256. Варто також зазначити, що організація процесу обміну текстовими повідомленнями у WhatsApp здійснюється на основі унікальної модифікації eXtensible Messaging & Presence Protocol, а саме FunXMPP. Для зберігання мультимедійного контенту WhatsApp використовує Yet Another Web Server. Останньою проаналізуємо внутрішню структуру Telegram та Telegram Mobile. Telegram відрізняється від Viber та WhatsApp тим, що практично всі дані користувача він зберігає на власних хмарних серверах, а не на кінцевому пристрою суб'єкта.

В якості бази даних месенджер використовує Telegram Database Library [6]. Telegram Database Library є власною розробкою компанії Telegram FZ-LLC. Ця база даних насправді є кросплатформною бібліотекою для створення додатків, схожих на Telegram. Telegram Database Library має наступні переваги: кросплатформеність, багатомовність (підтримує різні мови програмування), легкість у використанні (більшість важливих процесів автоматизовані), високий рівень продуктивності, узгодженість, надійність. Шифрування даних у месенджері Telegram реалізоване на основі власного протоколу компанії Telegram FZ-LLC – MTProto 2.0 [7]. Основою MTProto є оригінальна комбінація Advanced Encryption Standard (у режимі Infinite Garble Extension), протокол Діффі-Хеллмана (використовується для обміну 2048-бітними Rivest-Shamir-Adleman ключами), а також деякі хеш-функції (наприклад, SHA1 та SHA2). MTProto може використовуватися як в архітектурі «клієнт-сервер», так і для наскрізного шифрування.Іншими технологіями, які активно використовуються у месенджері, є Google Cloud Vision (аналіз контенту, закладеного у голосові повідомлення та графічні зображення), MessageBird (збір маркетингових даних) та Google Cloud Messaging (організація процесу обміну даними між хмарними серверами та клієнтським додатком).

В доповіді наводиться розроблена авторами криміналістична методика, за допомогою якої відбувався пошук та дослідження артефактів описаних вище месенджерів. Дана методика містить три основні частини: перелік директорій на користувацьких пристроях, де знаходяться артефакти месенджерів; перелік та опис внутрішньої структури цих артефактів; перелік програм та (або) скриптів, які потрібно використати під час вилучення (дослідження) артефактів. В стислому виді дану криміналістичну методику можна представити у вигляді таблиці 1.

Таблиця 1. Опис методики проведення криміналістичної експертизи месенджерів

Месенджер	Робочі директорії	Перелік артефактів	Використані програми та скрипти
Viber та Viber Mobile	Windows: C:\Users\"user"\AppData\Roaming\ViberPC\phone_number. Android: ..\Android\data\com.viber.voip\files; ..\data\data\com.viber.voip.	Windows: «viber.db», «data.db», «config.db»,» ..\Thumbnail,» «..\Avatars», «..\Icons», «..\Temporary». Android: «viber_message.db», «viber_data.db», «..\.image», «..\temp», «..\.ptt», «..\.video», «..\.thumbnails», «..\User photos».	SQLiteStudio
WhatsApp та WhatsApp Mobile	Windows: C:\Users\"user"\AppData\Local\Packages*.WhatsApp Desktop_*\LocalState;	Windows: «messages.db», «axolotl.db», «contacts.db», «settings.db», «..\Users\"user"\Downloads».	WhatsApp Viewer, WhatsApp Key Database Extractor Master [8].

Продовження таблиці 1

Месенджер	Робочі директорії	Перелік артефактів	Використані програми та скрипти
WhatsApp та WhatsApp Mobile	Windows: C:\Program Files\WindowsApps*.WhatsAppDesktop_*. Android: ..\Android\media\com.whatsapp\WhatsApp; ..\data\data\com.whatsapp\files\key.	Android: «msgstore.db.crypt14», «axolotl.db», «wa.db», «..\WhatsApp\Media»	WhatsApp Viewer, WhatsApp Key Database Extractor Master.
Telegram та Telegram Mobile	Windows: C:\Users\"user"\AppData\Roaming\Telegram Desktop; C:\Users\"user"\Downloads. Android: ..\Android\data\org.telegram.messenger\files; ..\Telegram.	Windows: «..\tdata», «..\Downloads». Android: «..\Pictures», «..\Telegram Images», «..\Telegram Video», «..\Telegram Audio», «..\Telegram Documents».	Telethon [9], Telegram analysis master, JSONViewer, OnlineDecoder.

У таблиці 1 представлено основні складові розробленої методики, яка використовувалася для проведення криміналістичної експертизи месенджерів Viber, WhatsApp та Telegram.

Дослідження артефактів, віднайдених за допомогою розробленої методики

Далі дослідимо внутрішню структуру артефактів, які було вилучено із месенджерів за допомогою раніше описаної методики. Почнемо з месенджера Viber.

Вище було сказано, що у Viber основними файлами, які містять найбільше інформації про користувача, є «viber.db» (Windows) та «viber_message.db» (Android). Ці файли мають схожу структуру. Серед артефактів, які в них можна знайти, є такі таблиці: «Calls» (здійснені голосові чи відеодзвінки), «DownloadFile» (скачані користувачем файли), «Events» (події, що відбулися всередині месенджера), «Messages» (текстові повідомлення, їх статус, часові мітки та інше), «Settings» (технічна інформація додатку: коли користувач останній раз був в онлайні, його дата ародження, операційна система, мова інтерфейсу, версія месенджера тощо); «UploadFile» (завантажені користувачем файли) та «Contact» (список контактів користувача).

У файлі «config.db» месенджера Viber можна знайти наступні артефакти (параметри): «ViberUserValue» (значення поточного користувача), «LauncherListenerPort» (використаний Viber порт), «Unblocker/...» (параметри блокувальника viber.db», «WindowGeometry» (розмір та координати вікна додатку Viber), «app-path» (місце розташування технічних файлів месенджера), «update-version» (поточна версія додатку), «ID» та «DeviceKey» (номер телефону власника облікового запису, а також ключ його пристрою).

Якщо ж говорити про те, як Viber працює з метаданими медіафайлів, то тут є одна особливість. У пересланих через Viber фотографій (або відео) зникають будь-які корисні метадані (наприклад, інформація про камеру або геодані) та змінюється розмір самого зображення. Крім цього, деякі медіафайли (наприклад, аватари користувачів), що зберігаються у локальному сховищі месенджера, не мають розширення, а тому їх неможна просто так відкрити у графічних редакторах або програвачах.

Наступними розглянемо артефакти месенджера WhatsApp. У WhatsApp найбільше артефактів знаходиться у файлах «messages.db» (Windows) та «msgstore.db.crypt14» (Android). До таких артефактів відносяться наступні таблиці: «call_log» (здійснені голосові чи відеодзвінки), «chat» (технічні дані чатів користувача), «jid» (список контактів користувача), «message» (текстові повідомлення, їх статус, часові мітки та інше), «props» (технічна інформація додатку, а також ім'я користувача, яке відображається в інтерфейсі), «message_media» (завантажені користувачем файли, а також ключ для скачування), «deleted_messages_view» (перелік видалених користувачем текстових повідомлень).

Файли «axolotl.db» та «wa.db» месенджера WhatsApp містять такий перелік таблиць-артефактів: «identities» (PublicKey та SecretKey користувача), «prekeys» (PreKeys для кожного чату користувача», «sessions» (інформація про активність користувача), «wa_block_list» (перелік заблокованих користувачем акаунтів), «wa_contacts» (список контактів користувача), «wa_trusted_contacts» (довірені контакти користувача), «group_membership_count» (перелік груп, членом яких є користувач), «wa_biz_profiles» (список бизнес-акаунтів WhatsApp).

Месенджер WhatsApp працює з метаданими медіафайлів наступним чином:

– месенджер приховує метадані файлів, що знаходяться у директорії ..\WhatsApp\Media;

– у пересланих через WhatsApp медіафайлів видаляється значна частина метаданих;

– метадані файлів можна у повній мірі побачити лише тоді, коли вони вручну переміщені на робочий стіл комп'ютера.

Останніми приведемо артефакти месенджера Telegram. Загалом, варто сказати, що, оскільки Telegram є хмарним месенджером, то на пристрої користувача він практично не залишає артефактів – тільки медіафайли. Перелік основних директорій, де зберігаються медіафайли, можна побачити у таблиці 1. У випадку з Telegram, медіафайли є досить корисним джерелом інформації, оскільки месенджер ніяк не видозмінює їх метадані. Таким чином, відкривши вікно властивостей медіафайлу, який зберігається у Telegram, можна побачити інформацію про пристрій користувача, геодані (де було зроблено фото/відео), а також інші персональні дані суб'єкта.

Також існує можливість викачати із серверів Telegram невеликий файл-базу даних, в якому записано перелік основних листувань користувача (текстові повідомлення разом з деякими персональними даними його співрозмовників). Щоб отримати цю базу даних, необхідно використати бібліотеку Telethon, написану для Python. Також варто додати, що деякі викачані таким способом файли будуть містити дані у форматі JSON, а тому для їх перегляду знадобиться відповідний редактор.

Підсумовуючи все зазначене вище, варто сказати, що, серед трьох досліджених месенджерів, найбільш захищеним з точки зору цифрової криміналістики є саме Telegram. По-перше, протокол шифрування, який використовується у Telegram (MTProto 2.0), у більшості випадків забезпечує кращій рівень захищеності та анонімності, ніж протоколи у Viber та WhatsApp. По-друге, оскільки Telegram практично повністю є хмарним месенджером, то він залишає на пристрої користувача найменшу кількість корисних артефактів (порівняно з Viber та WhatsApp).

Література

1. Рєзніченко Д.Ю. Методика цифрового криміналістичного дослідження месенджерів: зб. матеріалів учасн. XXVII Міжнар. молодіж. форуму. Т.4., м. Харків, ХНУРЕ, 10 – 12 трав. 2023 р., С. 98 – 99.

2. Рєзніченко Д.Ю. Методика проведення цифрової криміналістичної експертизи месенджерів: кваліфікац. робота бакалавра / Рєзніченко Димитрій Юрійович – Харків, ХНУРЕ, 2023. – 50 с.

3. Derek du Preez Viber migrates from MongoDB to Couchbase halves number of AWS servers [Електронний ресурс] // 2014. Режим доступу: https://diginomica.com/viber-migrates-mongodb-couchbase-halves-number-aws-servers.

4. Rakuten Viber Viber encryption overview [Електронний ресурс] // 2023. Режим доступу: https://www.viber.com/app/uploads/viber-encryption-overview.pdf.

5. Cosette C. Understanding WhatsApp's Architecture & System Design [Електронний ресурс] // 2021. Режим доступу: https://www.cometchat.com/blog/whatsapps-architecture-and-system-design.

6. TDLib [Електронний ресурс] // Режим доступу: https://core.telegram.org/tdlib/docs/.

7. End-to-End Encryption, Secret Chats [Електронний ресурс] // Режим доступу: https://core.telegram.org/api/end-to-end.

8. Yuvraj R. WhatsApp Key Database Extractor [Електронний ресурс] // 2021. Режим доступу: https://github.com/YuvrajRaghuvanshiS/WhatsApp-Key-Database-Extractor.

9. Telethon's Documentation [Електронний ресурс] // Режим доступу: https://docs.telethon. dev/en/stable/.