

Лабораторна робота: Артефакти месенджерів — Viber, Telegram

Артефакти Viber

1. Локації артефактів (Windows)

- C:\Users\"user"\AppData\Roaming\ViberPC\"phone_number\"
 - viber.db — основна БД з листуваннями, подіями, контактами
 - data.db, config.db — технічні параметри клієнта
 - Thumbnails, Avatars, Icons, Backgrounds, Temporary — медіа-каталоги

2. Ключові таблиці й поля у viber.db

- ChatInfo — перелік чатів, назви, токени останнього прочитаного, тема
- ChatRelation — відповідність ContactID ↔ ChatID; містить службові токени
- Contact — імена, номери телефонів, ідентифікатори завантажень, дати народження
- Calls — EventID, тип, тривалість, статус дзвінків
- DownloadFile — DownloadID, тимчасова назва, EventID, статус
- Events — події з TimeStamp, користувачами, токенами
- EventInfo — доповнення до Events: isRead, id стікерів, довжина повідомлення тощо
- Messages — текст у Body, статус, ThumbnailPath (шлях до зображення)
- Settings — платформа, мова, версія клієнта, LastOnlineTime, ін.
- Versions — історія версій застосунку

3. Особливості медіа та приватності (ПК)

- Thumbnails — знижена якість, без інформативних EXIF; дата створення часто дорівнює дню завантаження.
- Avatars — можуть зберігатися без розширення; для перегляду перейменувати у .jpg.

4. Завдання

- Знайти папку ViberPC з конкретним номером. Зробити скриншот вмісту кореня.
- Відкрити viber.db у SQLiteStudio і підготувати короткі описи з прикладами рядків для: ChatInfo, Contact, Messages, Events, Calls, DownloadFile, Settings.
- Витягнути з Thumbnails і Avatars по 2 файли, порівняти властивості, вказати відсутні/наявні метадані.
- Побудувати таймлайн для одного чату на основі Events або Messages за останні N подій.
- Зробити висновок, які артефакти найцінніші для атрибуції користувача та кореляції подій.

Артефакти Telegram

1. Локації артефактів (Windows)

- C:\Users\%user%\AppData\Roaming\Telegram Desktop\
 - tdata — зашифровані файли сесій і налаштувань (settingss), кеш для секретних чатів (user_data\media_cache), службові ключові файли
- C:\Users\%user%\Downloads\Telegram Desktop — завантажені користувачем файли

2. Що зберігається і як аналізувати на ПК

- tdata — напряду нечитабельна без ключів; однак часові мітки й факт наявності файлів мають доказове значення (вказують на активність клієнта).
- Офіційний експорт: Settings → Advanced → Export Telegram data — дозволяє отримати локальний набір чатів і медіа у зрозумілому форматі (HTML/JSON), зручний для аналізу на ПК.

- Результати через Telethon (за наявності облікових даних і API-токена):
 - Your-Telegram-Username.db — SQLite із таблицями entities, sent_files, sessions, versions, update_state
 - channel_messages.json — перелік повідомлень у JSON із текстом, датами, авторами й вкладеннями

3. Особливості медіа на ПК

- У Downloads\Telegram Desktop медіафайли часто не містять багатих EXIF. Властивості ОС показують базові поля (дату запису, розмір, роздільність для зображень тощо).

4. Завдання

- Знайти tdata та каталог Downloads\Telegram Desktop. Зробити скриншоти структури.
- Виконати офіційний Export Telegram data з одного невеликого чату. Додати у звіт приклади файлів та коротко описати структуру експорту.
- За наявності Telethon-дампу: у Your-Telegram-Username.db виписати з entities 3 записи з полями username, phone, дата останньої взаємодії; з channel_messages.json відновити читабельний текст 3 повідомлень і часові мітки.
- Порівняти інформативність офіційного експорту й Telethon-дампу для задач атрибуції та встановлення фактів спілкування.