Технічні науки

УДК 004.65

Бичков Сергій Олександрович

заступник завідувача відділу комп'ютерно-технічних та телекомунікаційних досліджень

Харківський науково-дослідний експертно-криміналістичний центр МВС України

Bychkov Serhii

Department of Digital Forensics Semi-Head

Kharkiv Scientific Research Forensic Center of MIA of Ukraine

КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ ЗАСТОСУНКУ OLX™ НА ПРИСТРОЯХ З ОПЕРАЦІЙНОЮ СИСТЕМОЮ ANDROID

FORENSIC INVESTIGATION OF THE OLX APPLICATION ON ANDROID DEVICES

Анотація. *Вступ. В комп'ютерній криміналістиці вилучення листування користувача у мобільних застосунках є доволі важливим аспектом при розслідуванні кримінальних правопорушень. На сьогоднішній день існує велике різноманіття мобільних застосунків, де листування є не основною функцією таких мобільних застосунків. Як приклад, мобільні застосунки відомих в Україні торгівельних майданчиків або маркетплейсів «Розетка™», «OLX™», «Алло™» та інших. Підтримка вилучення листування із зазначених мобільних застосунків програмним забезпеченням для вилучення та криміналістичного аналізу даних з мобільних пристроїв на сьогоднішній день відсутня. Це, ймовірно, обумовлено їх локалізацією в окремих регіонах та незначним поширенням на мировому ринку, оскільки товари та послуги, які вони пропонують, призначені для цільової аудиторії користувачів з України. Для прикладу вилучення листування у схожому за*

функціоналом мобільному застосунку «Aliexpress®» торгівельного майданчика з аналогічною назвою, але товари якої мають глобальне поширення підтримується програмним забезпеченням «Oxygen Forensic® Detective».

Мета. Метою дослідження є аналіз встановленого мобільного застосунку «OLX™» на пристроях під керуванням операційної системи «Android» з метою виявлення відомостей щодо об'яв або листування в них. Для пошуку даних застосовувалось спеціальне програмне забезпечення призначене для криміналістичного аналізу даних збережених в пам'яті мобільних пристроїв, що використовується судовими експертами при проведенні судових комп'ютерно-технічних експертиз.

Результати. В результаті проведених досліджень, виявлено два файли баз даних «ChatSellingDb.db» та «ChatBuyingDb.db» полегшеної реляційної системи керування базами даних – SQLite. Файл бази даних «ChatSellingDb.db» містить 3 таблиці: android_metadata, ChatListItem та room_master_table. Таблиця «ChatListItem» відповідає за збереження записів щодо листування у об'явах, створених безпосередньо користувачем мобільного застосунку «OLX». Файл бази даних «ChatBuyingDb.db» містить також 3 таблиці з аналогічними назвами, таблиця «ChatListItem» якої відповідає за збереження записів щодо листування у об'явах створених користувачами, які пропонують свої послуги та товари засобами мобільного застосунку «OLX». Виявлені файли розташовані в операційній системи Android за шляхом «/data/data/ua.slando/databases/».

Перспективи. В подальшому планується розробка SQL-запитів [1, с. 57] до виявлених файлів баз даних. Результатом виконання зазначених SQL-запитів повинна бути таблиця, яка містить інформацію щодо об'яви, в якій відбувається листування, інформацію щодо змісту листування, інформацію про учасників листування.

Ключові слова. *OLX, експертиза, форензіка, комп'ютерна експертиза, база даних.*

Summary. *In computer forensics, extracting user chating from mobile applications is a critical aspect of investigating criminal offenses. Currently, there is a wide variety of mobile applications where messaging is not a primary function. Examples include mobile applications of well-known Ukrainian marketplaces such as «Rozetka™», «OLX™», «Allo™» and others. Support for extracting correspondence from these applications using software tools for data acquisition and forensic analysis of mobile devices is currently unavailable. This is likely due to the limited international presence of these applications, as the goods and services they offer are primarily targeted at users in Ukraine. For instance, correspondence extraction is supported for a similar application, «Aliexpress®» a global marketplace with a comparable function, using the «Oxygen Forensic® Detective» software.*

Key words: *OLX, expertise, forensics, computer forensics, database.*

Постановка проблеми. Звертаючи увагу на те, що при проведенні судових комп'ютерно-технічних експертиз по мобільним пристроям відповідно до методичних рекомендацій [2, с. 17] та світової практики експерт працює з об'єктом дослідження ізольованим від підключення до мереж передачі даних та мобільного зв'язку, тобто переведеним в авіарежим (в залежності від виробника мобільного пристрою назва цього режиму може відрізнятись), то отримати необхідні дані візуальним дослідженням з мобільних застосунків, які потребують обов'язкового з'єднання з мережею Інтернет не є можливим. Мобільний застосунок «OLX™» саме і відноситься до таких, що потребують обов'язкового підключення до мережі Інтернет для роботи з ним та перегляду інформації про існуючи об'яви або листування продавцем/покупцем.

Оскільки існує певна категорія кримінальних правопорушень – злочинів, передбачених статтею 190 «Шахрайство» Кримінального кодексу України [3], здійснення яких відбувається із використанням сервісу «OLX™», то перед судовим експертом постає задача у видобуванні даних про об'яви та листування у мобільному застосунку «OLX™» з мобільних пристроїв потерпілих або підозрюваних у скоєнні злочину.

Виклад основного матеріалу. Для проведення дослідження був обраний мобільний телефон торгової марки «Samsung», модель Galaxy A50 SM-A505FM/DS, розмір вбудованої пам'яті для зберігання даних – 120 Гб, розмір ОЗУ – 6 Гб.

Обраний мобільний телефон має такі характеристики програмного забезпечення:

- операційна система Android 11,
- версія інтерфейсу користувача One UI 3.1,
- версія програмного забезпечення (прошивка) – A505FXXS9CVL1,
- версія Knox – 3.7,
- рівень патчу безпеки Android – 01.01.2023,
- root-доступ – відсутній.

Для виготовлення копії даних з вбудованої пам'яті мобільного телефона використовувався програмно-апаратний комплекс «Cellebrite UFED Touch 2», версія прошивки – 7.72.0.48. Для дослідження даних, що зберігає мобільний застосунок, необхідно отримати копію вбудованої пам'яті мобільного пристрою, яка містить дані із захищеної області даних операційної системи Android. Привілеїв доступу, які надаються звичайному користувачу операційної системи, недостатньо для доступу до таких даних. Таким чином, на момент проведення дослідження існує три доступних методи для виготовлення копії, яка буде містити потрібні дані, а саме:

1) фізична копія пам'яті пристроїв на базі процесорів сімейства Exynos (найповніша);

2) розширена логічна копія файлової системи, що вилучається на запущеній операційній системі пристрою (із застосуванням Live-методів, які доступні лише у програмному забезпеченні та програмно-апаратних комплексах компанії «Cellebrite»);

3) копія файлової системи, якщо в операційній системі отримано root-доступ.

Для виготовлення копії даних був обраний метод розширеної логічної копії файлової системи програмно-апаратного комплексу «Cellebrite UFED Touch 2» – «Exynos Live». Метод виготовлення копії файлової системи з відкритим root-доступом не застосовувався в зв'язку з ймовірністю повної втрати даних користувача. Обробка та аналіз виготовленої копії даних проводився у програмному забезпеченні «Oxygen Forensic® Detective», версії 17.0.0.282.

В результаті проведеного дослідження виявлено два файли розташовані за шляхом /data/data/ua.slando/databases/. Файл бази даних «ChatSellingDb.db» містить 3 таблиці: android_metadata, ChatListItem та room_master_table. Таблиця «ChatListItem» відповідає за збереження записів щодо листування у об'явах створених безпосередньо користувачем мобільного застосунку «OLX». Файл бази даних «ChatBuyingDb.db» містить також 3 таблиці з аналогічними назвами, таблиця «ChatListItem» якої відповідає за збереження записів щодо листування у об'явах створених користувачами, які пропонують свої послуги та товари засобами мобільного застосунку «OLX».

Таблиця «ChatListItem» файлу бази даних «ChatSellingDb.db», містить такі дані: інформацію щодо змісту повідомлень у об'явах, ID-номери об'яв, назви об'яв, ID-номери покупців, ID-номери власника об'яви, дати та часу повідомлень.

Таблиця «ChatListItem» має таку структуру:

- рядок – чат з окремим користувачем в конкретній об'яві;
- стовпчик «primaryKey» – унікальний номер запису в базі даних, значення має вигляд «a60f916e-5752-4c06-9672-25876532b3e4»;
- стовпчик «id» – унікальний номер першого повідомлення від конкретного покупця в об'яві, значення має вигляд «a60f916e-5752-4c06-9672-25876532b3e4» (відповідає унікальному номеру запису в базі даних «primaryKey»);
- стовпчик «ad» – містить інформацію про об'яву, значення має вигляд «{"id":"794873794","title":"Видеокарта MSI GTX1080TI на 11GB (11264MB)","category":{"type":"electronics"},"active":true}», де:
  - id – унікальний номер об'яви,
  - title – назва об'яви,
  - category – категорія об'яви,
  - active – стан (активна чи ні).
- стовпчик «respondent» – інформація про покупця, значення має вигляд «{"id":"375113849","name":"shekhoor","type":"BUYER","blocked":false}», де:
  - id – унікальний номер користувача,
  - name – ім'я користувача,
  - type – тип користувача (у даному випадку «BUYER» – покупець),
  - blocked – статус (заблокований чи ні).
- стовпчик «timestamp» – дата та час останнього повідомлення в чаті,
- стовпчик «adimageurl» – посилання на титульне зображення об'яви,

- стовпчик «messages» – чат з покупцем у конкретній об'яві. Містить листування двох осіб: покупця та продавця, які унікально ідентифікуються полем «user_id». Значення поля «user_id» покупця дорівнює полю «id» покупця з стовпчика «respondent». Приклад вигляду даних комірки з стовпчику «messages» наведений на рисунку 1. Дані представлені у текстовому форматі JSON [4, с. 187].

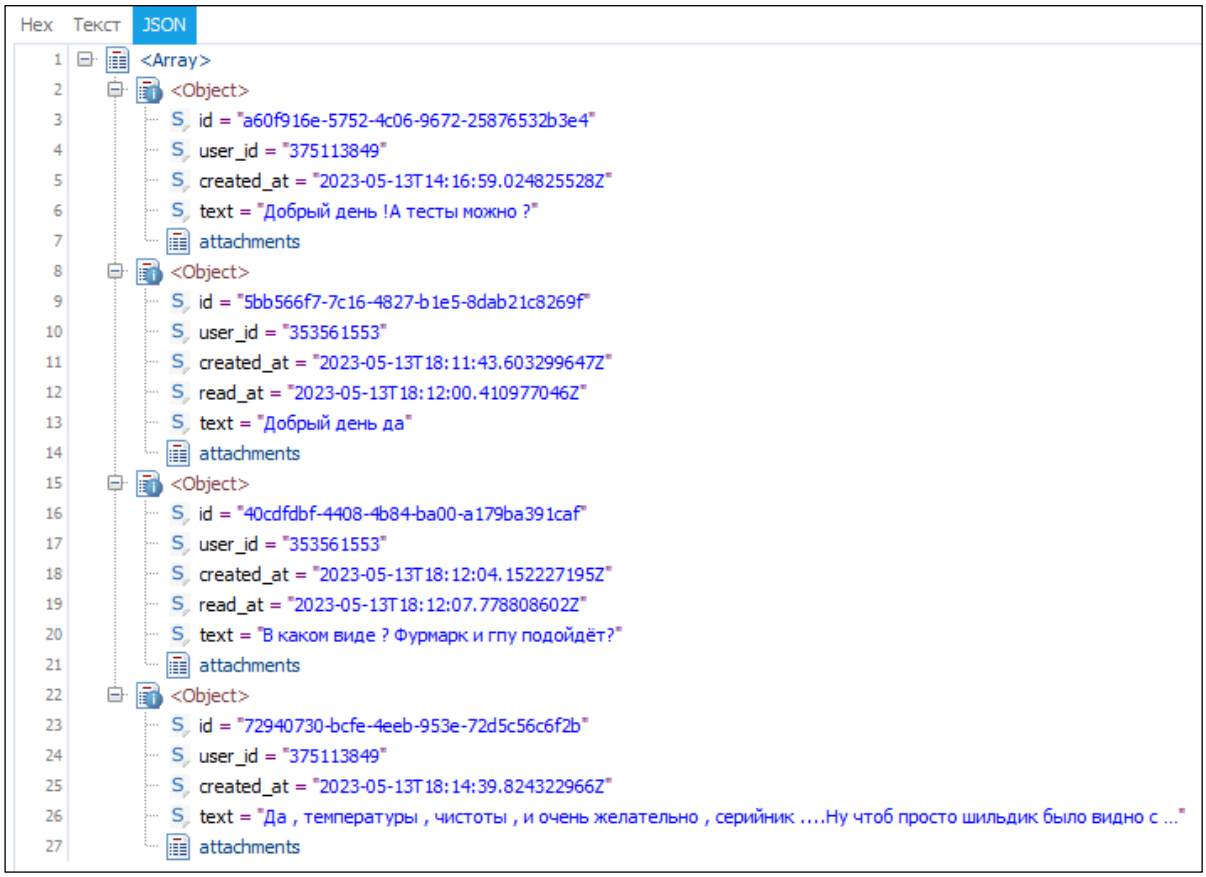

Рис. 1. Приклад вигляду даних комірки з стовпчику «messages» таблиці «ChatListItem» файлу бази даних «ChatSellingDb.db»

де:

- id – унікальний номер повідомлення,
- user_id – унікальний номер користувача (user_id покупця дорівнює id покупця з стовпчика «respondent»),
- created_at – дата та час створення повідомлення,
- text – текст повідомлення,
- read_at – дата та час коли повідомлення було прочитано,

- attachments – інформація про вкладення.

Таким чином, в результаті проведених досліджень, виявлено два файли баз даних «ChatSellingDb.db» та «ChatBuyingDb.db» полегшеної реляційної системи керування базами даних – SQLite. Файл бази даних «ChatSellingDb.db» містить 3 таблиці: android_metadata, ChatListItem та room_master_table. Таблиця «ChatListItem» відповідає за збереження записів щодо листування у об'явах, створених безпосередньо користувачем мобільного застосунку «OLX». Файл бази даних «ChatBuyingDb.db» містить також 3 таблиці з аналогічними назвами. Таблиця «ChatListItem» бази даних «ChatBuyingDb.db» відповідає за збереження записів щодо листування у об'явах, створених користувачами, які пропонують свої послуги та товари засобами мобільного застосунку «OLX». Виявлені файли розташовані в операційній системи Android за шляхом «/data/data/ua.slando/databases/».

В подальшому планується розробка SQL-запитів до виявлених файлів баз даних. Результатом виконання зазначених SQL-запитів повинна бути таблиця, яка містить інформацію щодо об'яви, в якій відбувається листування, інформацію щодо змісту листування, інформацію про учасників листування. Також перспективним залишається дослідження наявності видалених записів в виявлених файлах баз даних.

Література

1. В'єскас Дж., Ернандес М. Дж. SQL Queries for Mere Mortals: A Hands-On Guide to Data Manipulation in SQL. Вид. 3. Бостон : Addison-Wesley, 2014. 800 с.

2. Дослідження мобільних пристроїв під керуванням операційної системи Android : метод. рек. / уклад. В. А. Поліщук. К. : ДНДЕКЦ МВС України, 2017. 22 с.

3. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 16.12.2024).

4. Фрізен Д. Java XML and JSON: Document Processing for Java SE. Вид. 2. Дофін : Apress, 2019. 528 с.