МКО
СИСТЕМЫ

ИСПОЛЬЗОВАНИЕ ЖУРНАЛОВ БАЗ ДАННЫХ SQLITE ПРИ РАССЛЕДОВАНИИ ЦИФРОВЫХ ИНЦИДЕНТОВ

ЖУРНАЛ SQLITE – «ЧЕРНЫЙ ЯЩИК» БАЗЫ ДАННЫХ

1. Что хранится в базах данных
2. Удалено из базы ≠ исчезло бесследно
3. Практические кейсы расследований

ПОЧЕМУ ИМЕННО SQLITE?

РАСПРОСТРАНЕННАЯ ВСТРОЕННАЯ СУБД ДЛЯ ANDROID, iOS, macOS, WINDOWS, LINUX

- Не требует отдельного сервера
- Почти не требует настройки
- Хранит данные в обычных файлах
- Высокая производительность при малом размере

ЧТО ХРАНИТСЯ?

- Сообщения
- Данные о местоположении
- История браузера
- Сведения банковских приложений
- Контакты
- Настройки и служебные данные
- Журналы вызовов

ЖУРНАЛЫ SQLITE НЕРЕДКО СОХРАНЯЮТ СЛЕДЫ ИЗМЕНЕНИЙ ДАЖЕ ПОСЛЕ ИХ УДАЛЕНИЯ ИЗ ОСНОВНОЙ БАЗЫ ДАННЫХ

1 **СООБЩЕНИЕ**
отправлено

2 **ПРАВКА**
18:00 → 18:10

3 **УДАЛЕНИЕ**
запись исчезает

DATABASE.DB
только итоговое состояние

≠

ЖУРНАЛЫ SQLITE
могут сохранить следы изменений

МЕХАНИЗМ WAL:
СНАЧАЛА ЖУРНАЛ, ПОТОМ БАЗА

APP
создает / меняет / удаляет запись

DATABASE-WAL
изменение сначала попадает сюда

CHECKPOINT
переносит изменения

DATABASE.DB
актуальное состояние

DATABASE.DB
актуальные данные

DATABASE-WAL
журнал изменений

DATABASE-SHM
служебная информация

В ЖУРНАЛЕ WAL МОГУТ СОДЕРЖАТЬСЯ

Новые записи	еще не перенесенные в database.db
Удаленные записи	следы объектов, исчезнувших из основной БД
Предыдущие версии	состояния измененных данных
Временные состояния	промежуточные варианты базы
Незавершенные транзакции	события, которые не дошли до checkpoint

ПРОСТОЙ ПРИМЕР: ОДНО СООБЩЕНИЕ – ТРИ СОСТОЯНИЯ В WAL

1 **18:00**
Встречаемся в 18:00

2 **19:00**
Встречаемся в 19:00

3 **DELETE**
Сообщение удалено

ТРИ ИНЦИДЕНТА О НЕЗАКОННОМ ОФОРМЛЕНИИ КРЕДИТОВ

№	Потерпевший	Дата	Сумма	Устройство	Метод МК
A	Иванов И.И.	12.11.2025	11 000	Tecno Spark 8C (Tecno KG5n)	Unisoc / Spreadtrum Android
B	Петров П.П.	13.01.2025	34 000	Samsung Galaxy M12 (SM-M127F)	Полная файловая система
C	Сидоров С.С.	25.01.2026	23 000	Realme Note 50 (RMX3834)	Unisoc / Spreadtrum Android

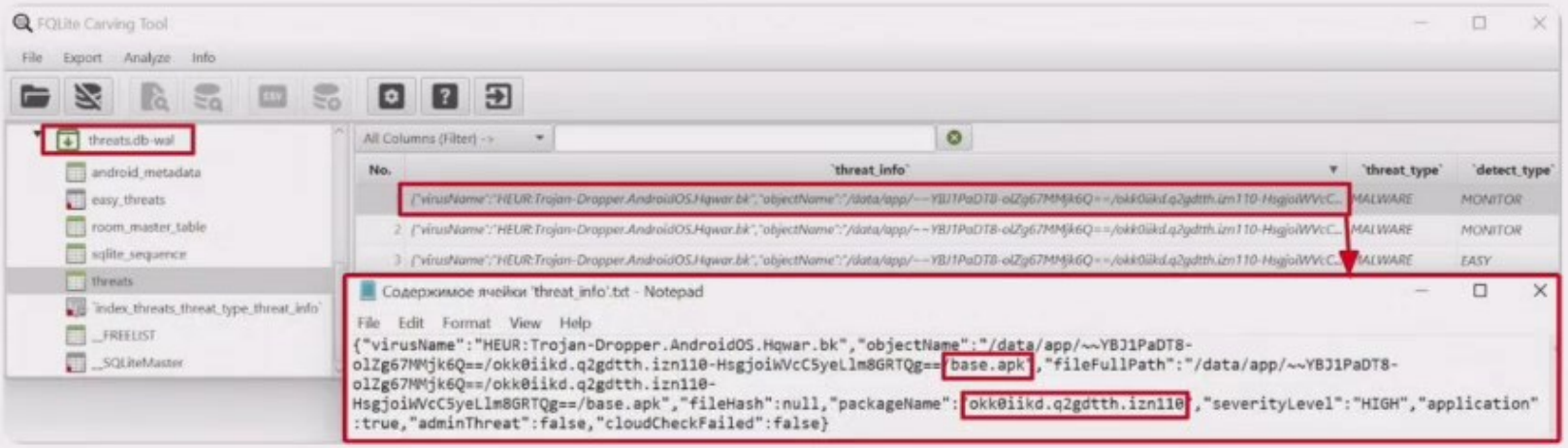
ИНЦИДЕНТ А:

«ПОИСК ПО ФИО БП»

ОБНАРУЖЕНИЕ СЛЕДОВ ВРЕДОНОСНОГО ПО

ИНЦИДЕНТ А

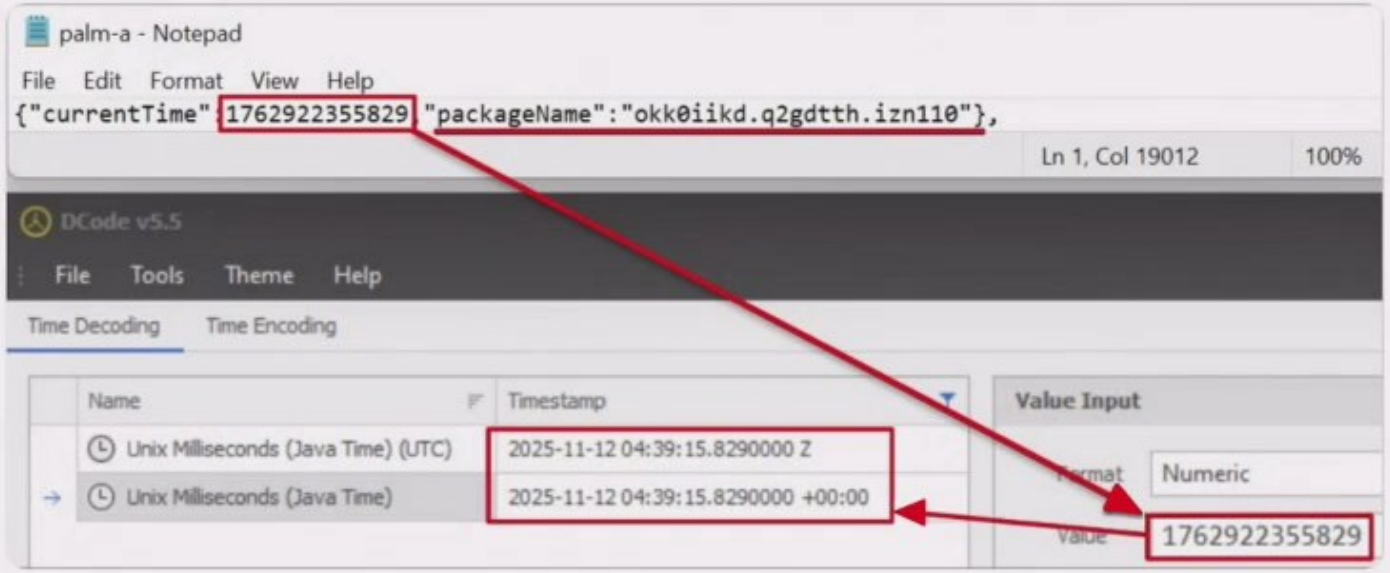
В журнале **threats.db-wal** приложения «СберБанк Онлайн» обнаружена запись о **base.apk,** который встроенный антивирусный модуль определил как **HEUR:Trojan-Dropper.AndroidOS.Hqwar.bk.** Сам файл уже отсутствовал, но сохранился его идентификатор **okk0iikd.q2gdtth.izn110**



ПОДТВЕРЖДЕНИЕ УСТАНОВКИ ПРИЛОЖЕНИЯ

ИНЦИДЕНТ А

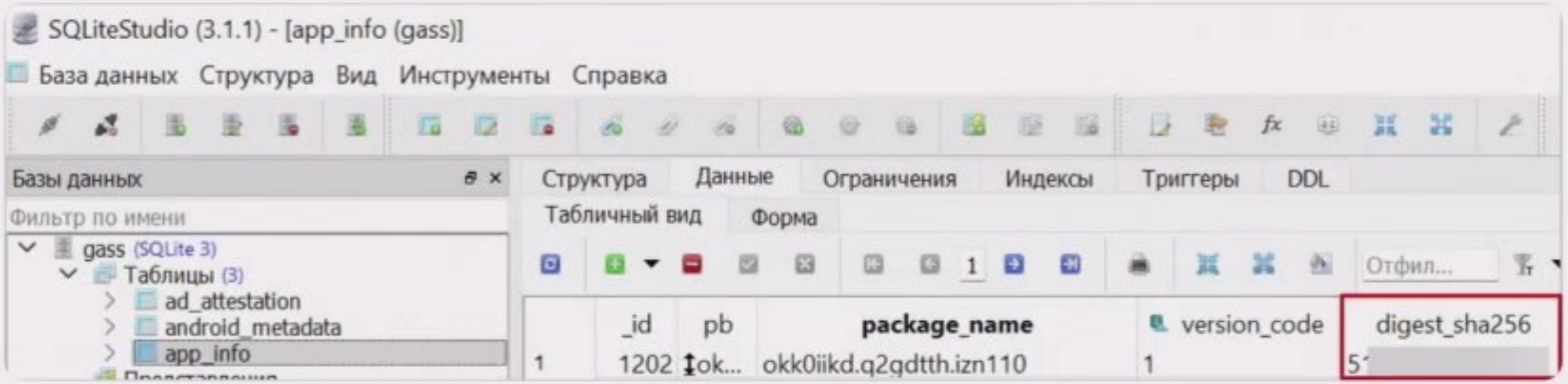
В файле **packages.xml** записей о приложении с идентификатором **okk0iikd.q2gdtth.izn110** не обнаружено, однако служебный журнал **palm-a** сохранил событие его регистрации **12.11.2025** в **04:39:15**



ПОЛУЧЕНИЕ ЦИФРОВОГО «ОТПЕЧАТКА»

ИНЦИДЕНТ А

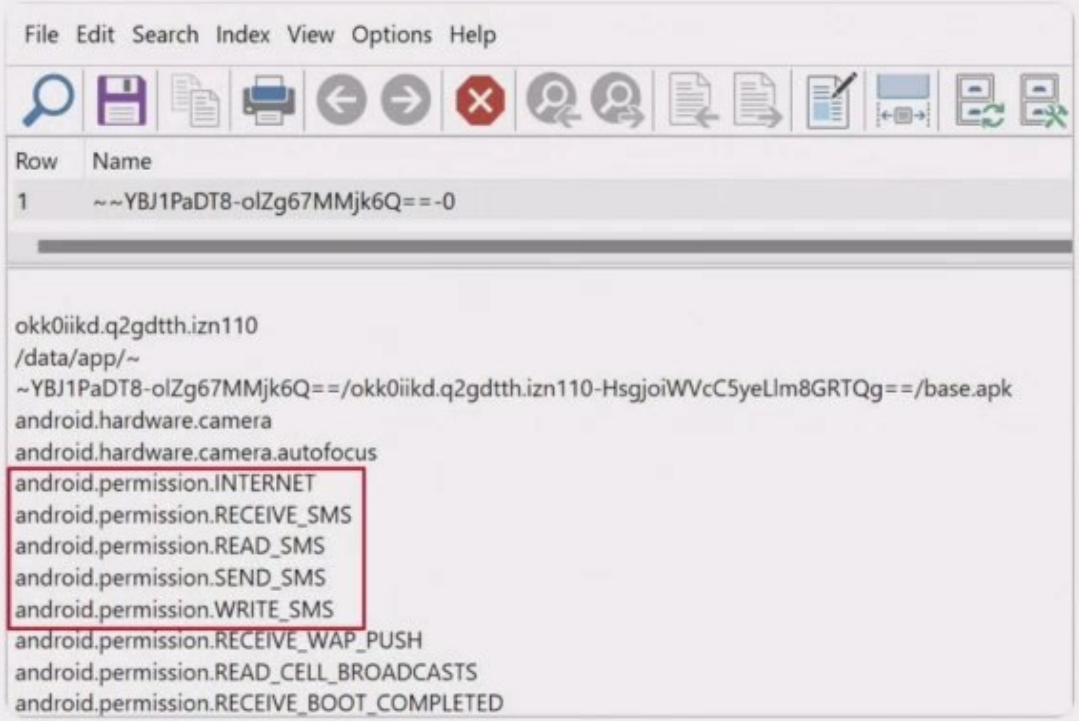
В системной базе данных **gass.db** сохранилась контрольная сумма (алгоритм вычисления – SHA256) установочного файла приложения с идентификатором **okk0iikd.q2gdtth.izn110**



КАКИЕ ВОЗМОЖНОСТИ ИМЕЛО ПРИЛОЖЕНИЕ

ИНЦИДЕНТ А

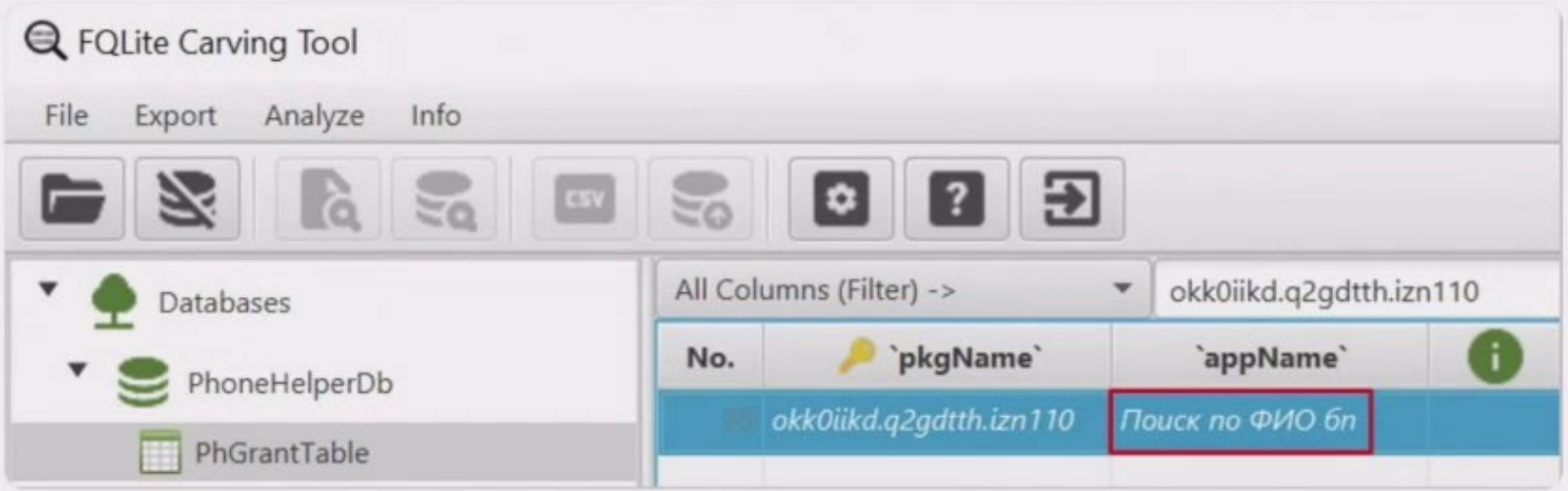
В файле **AndroidManifest.xml** содержалась информация о разрешениях, которые приложение с идентификатором **okk0iikd.q2gdtth.izn110** запрашивало у ОС Android: **подключение к сети Интернет, получение и отправка SMS-сообщений**



ОТОБРАЖАЕМОЕ ИМЯ ПРИЛОЖЕНИЯ

ИНЦИДЕНТ А

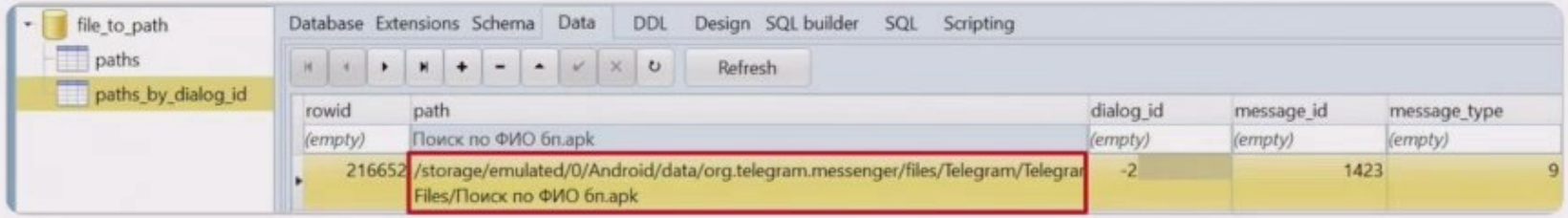
Из файла **PhoneHelper.Db** установлено, что приложение с идентификатором **okk0iikd.q2gdtth.izn110** отображалось на устройстве под именем **«Поиск по ФИО бп»**



КАК ПРИЛОЖЕНИЕ ПОПАЛО НА УСТРОЙСТВО

ИНЦИДЕНТ А

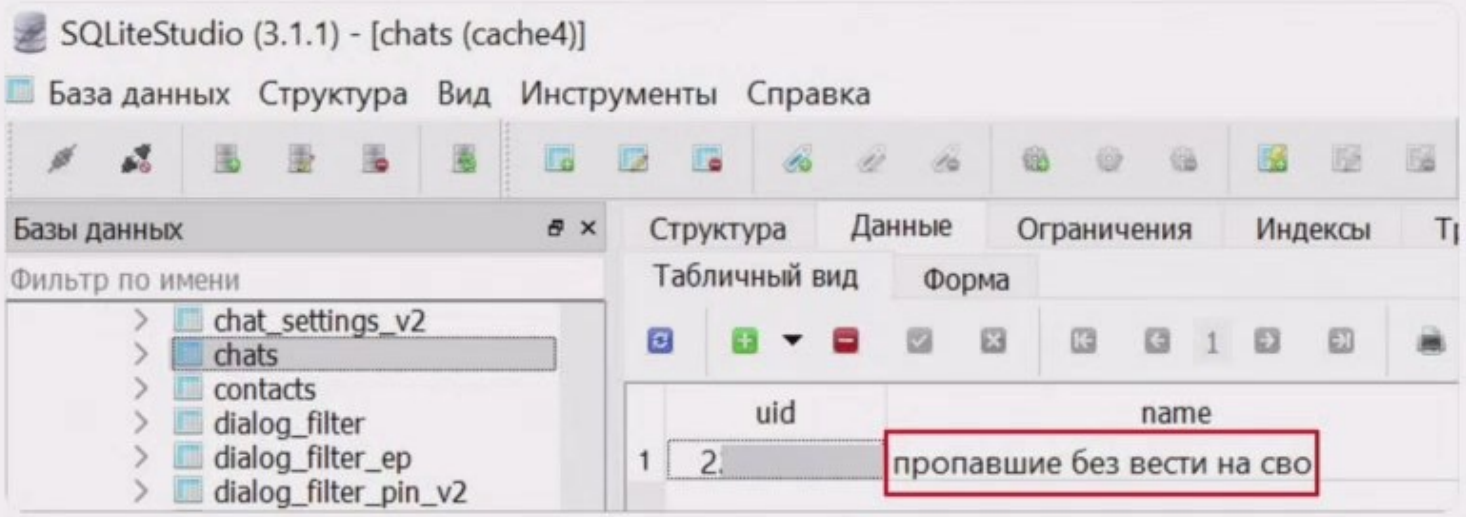
В базе данных **file_to_path.db** мессенджера **Telegram** обнаружена запись о получении файла **«Поиск по ФИО бп.apk»** в одном из чатов



ЧТО УДАЛОСЬ УЗНАТЬ О ЧАТЕ TELEGRAM

ИНЦИДЕНТ А

При исследовании мессенджера Telegram сообщения в таблице **messages_v2** отсутствовали, однако в таблице **chats** сохранилась информация о названии чата: **«пропавшие без вести на сво»**



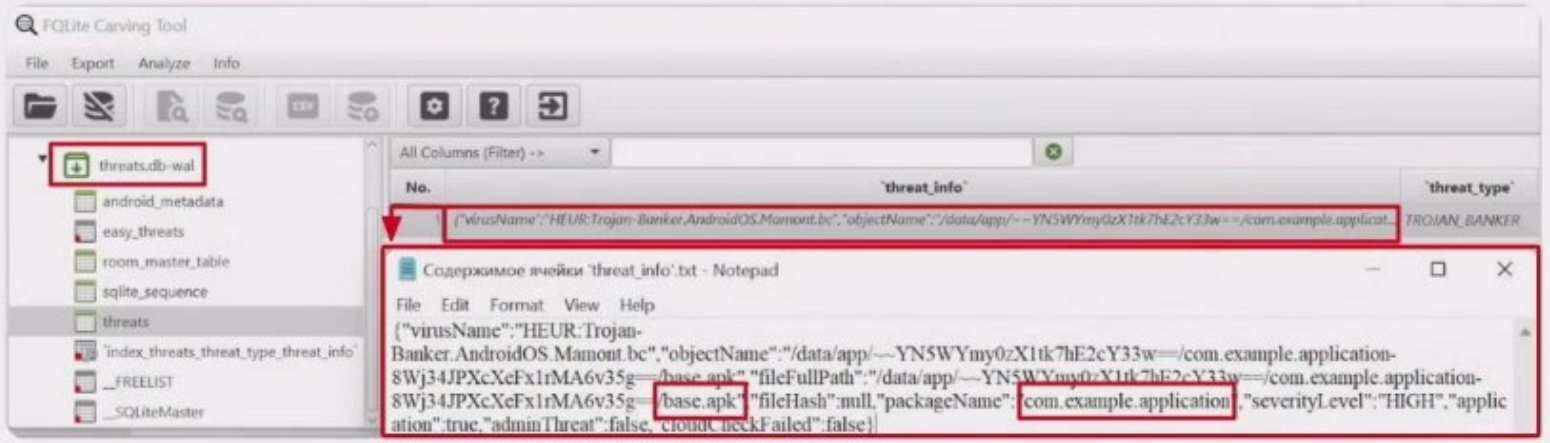
ИНЦИДЕНТ В:

«PHOTO ARCHIVE (20)»

ОБНАРУЖЕНИЕ СЛЕДОВ ВРЕДОНОСНОГО ПО

ИНЦИДЕНТ В

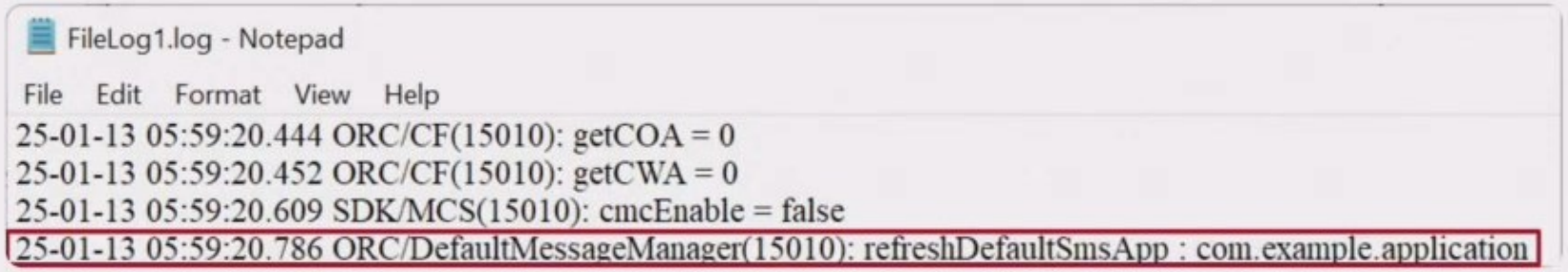
В журнале **threats.db-wal** приложения «СберБанк Онлайн» сохранилась запись о **base.apk**, который встроенный антивирусный модуль определил как **HEUR:Trojan-Banker.AndroidOS.Mamont.bc.** Сам файл уже отсутствовал, но в журнале сохранился его идентификатор **com.example.application**



КАКИЕ ВОЗМОЖНОСТИ ИМЕЛО ПРИЛОЖЕНИЕ

ИНЦИДЕНТ В

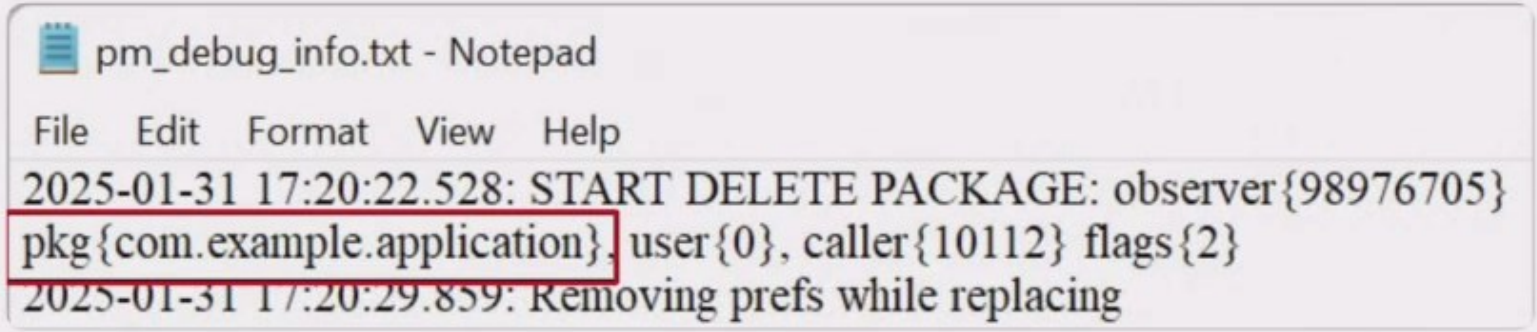
Анализ журнала **FileLog1.log** подтвердил, что 1**3.01.2025 в 05:59:20** приложение с идентификатором com.example.application было назначено стандартным приложением для работы с SMS



ПОДТВЕРЖДЕНИЕ УДАЛЕНИЯ ПРИЛОЖЕНИЯ

ИНЦИДЕНТ В

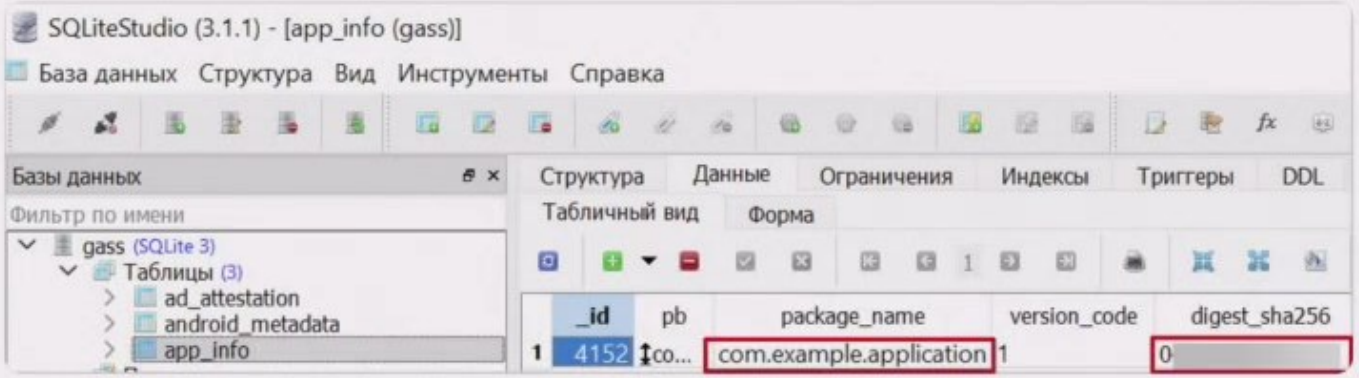
Анализ файла **pm_debug_info.txt** подтвердил удаление приложения с идентификатором **com.example.application: 31.01.2025 в 17:20:22**

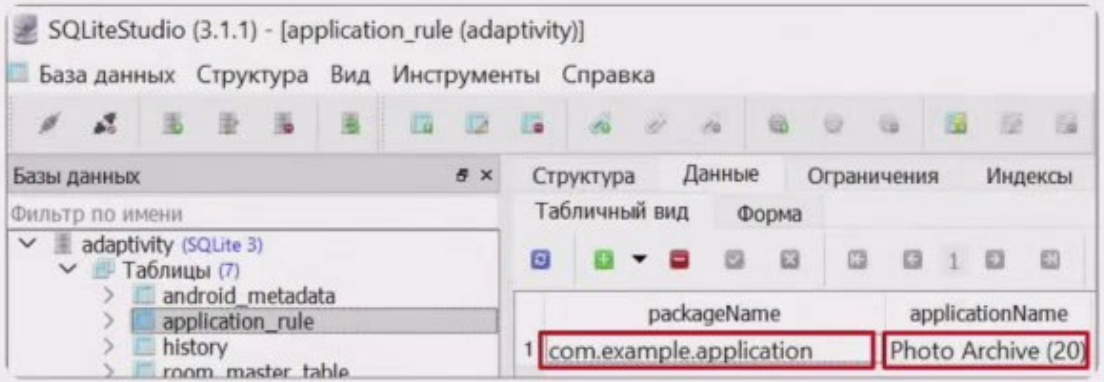


ЦИФРОВОЙ «ОТПЕЧАТОК» И ОТОБРАЖАЕМОЕ ИМЯ ПРИЛОЖЕНИЯ. ИСТОЧНИК ПОЛУЧЕНИЯ АРК-ФАЙЛА

ИНЦИДЕНТ В

- В системной базе данных **gass.db** сохранилась контрольная сумма (алгоритм вычисления – SHA256) установочного файла приложения с идентификатором **com.example.application**
- Файл служебной базы данных антивирусного ПО **adaptivity.db** сохранил информацию об отображаемом имени приложения – **«Photo Archive (20)»**
- В базе данных cache4.db мессенджера Telegram была обнаружена запись о получении файла **Photo Archive (20).apk** в одном из чатов





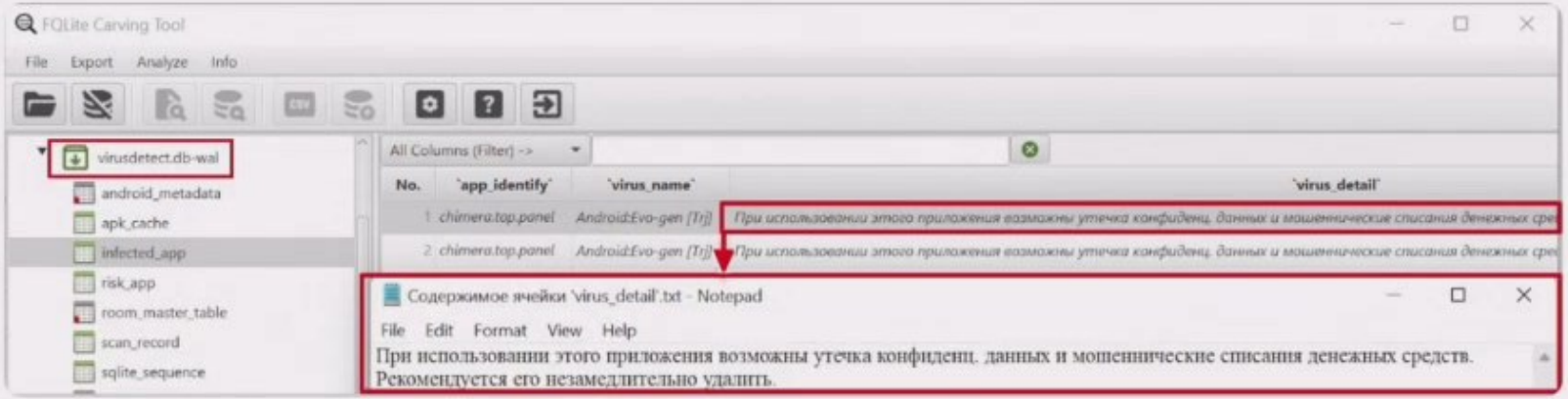
ИНЦИДЕНТ В:

«ВИДЕО.ЧП(3)»

ОБНАРУЖЕНИЕ СЛЕДОВ ВРЕДОНОСНОГО ПО

ИНЦИДЕНТ С

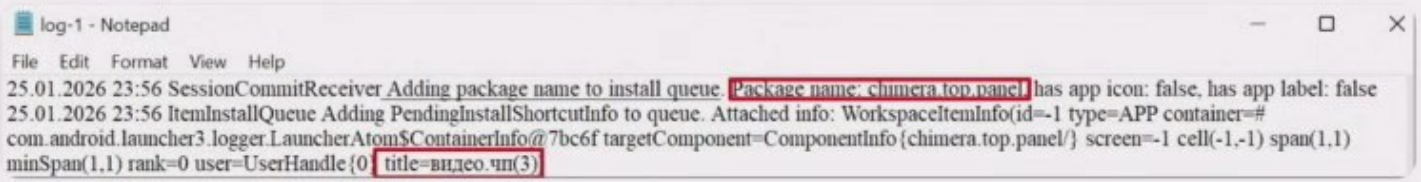
В журнале **virusdetect.db-wal** обнаружена запись о приложении **chimera.top.panel,** которое встроенный антивирус классифицировал как **Android:Evo-gen [Trj].** Журнал также содержал предупреждение о риске утечки конфиденциальных данных и мошеннического списания денежных средств

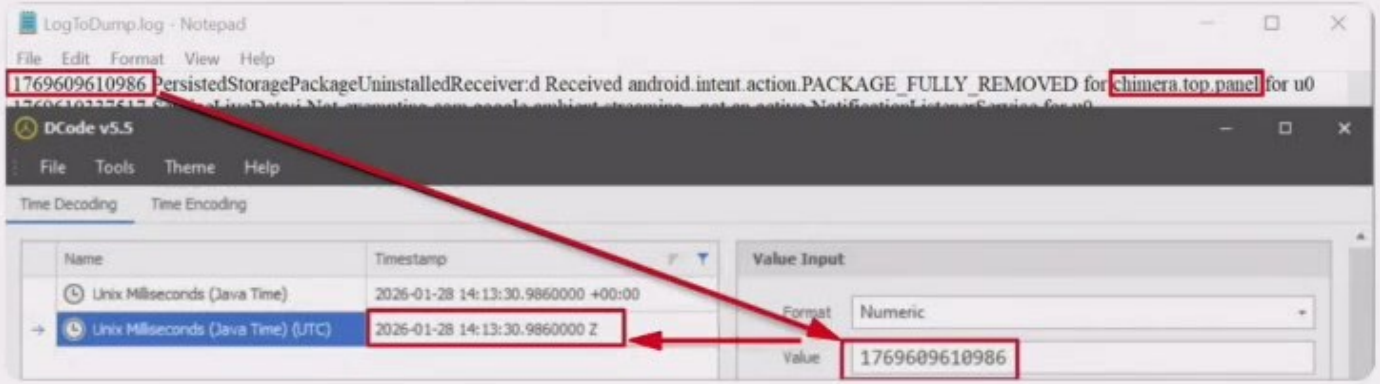


ПОДТВЕРЖДЕНИЕ УСТАНОВКИ И УДАЛЕНИЯ ПРИЛОЖЕНИЯ

ИНЦИДЕНТ С

- В журнале **log-1** обнаружена запись об установке приложения **chimera.top.panel 25.01.2026 в 23:56** и его отображаемое имя – «видео.чп(3)»
- Журнал **LogToDump.log** подтвердил удаление этого приложения **28.01.2026 в 14:13:30**

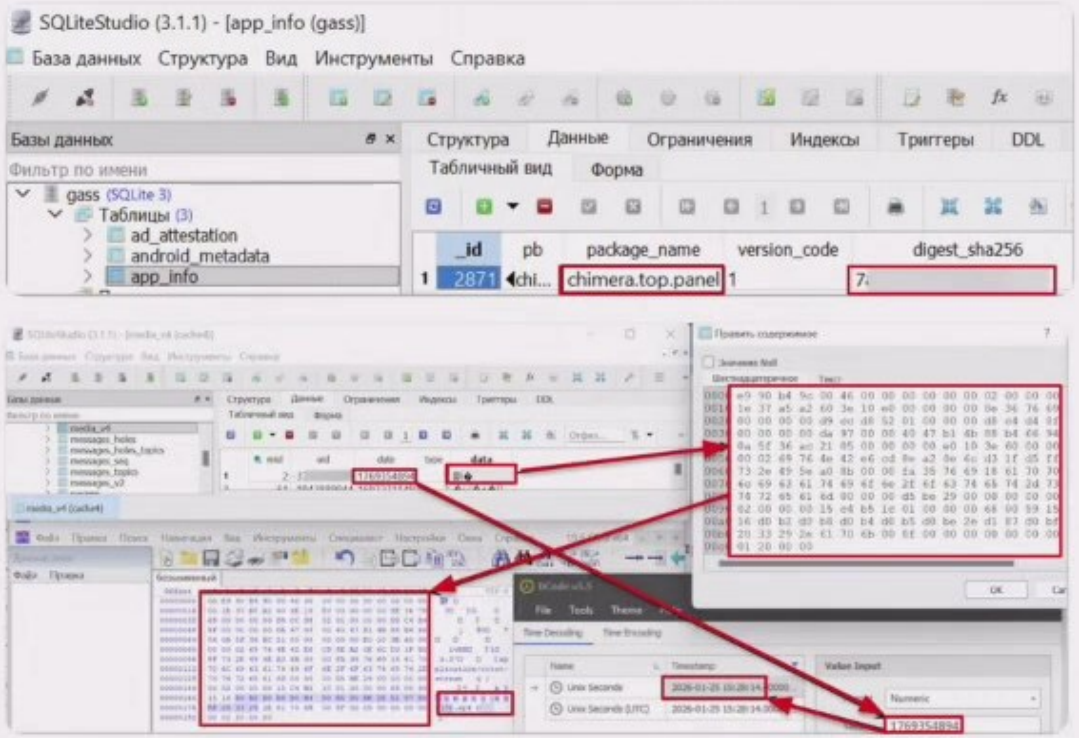




ЦИФРОВОЙ «ОТПЕЧАТОК» И ИСТОЧНИК ПОЛУЧЕНИЯ АРК-ФАЙЛА

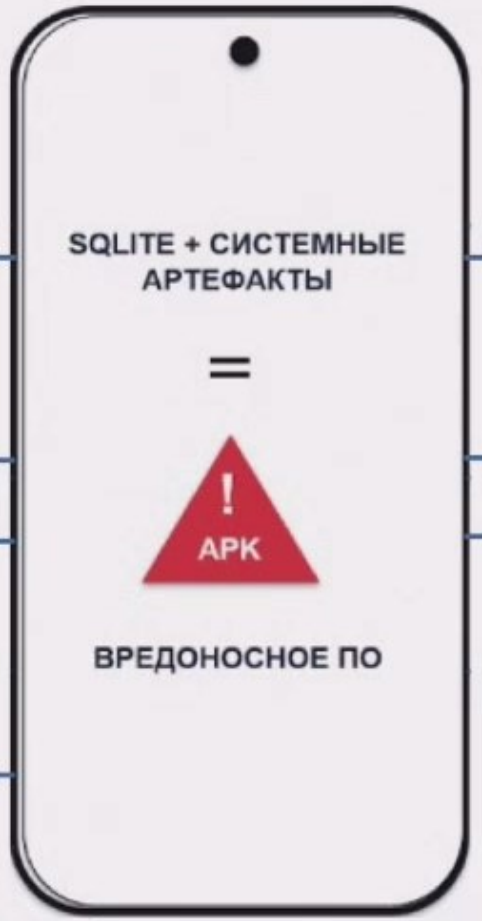
ИНЦИДЕНТ С

- В системной базе данных **gass.db** сохранилась контрольная сумма (алгоритм вычисления – SHA256) установочного файла приложения с идентификатором **chimera.top.panel**
- В базе данных **cache4.db** мессенджера **Telegram** обнаружена запись о получении файла **«видео.чп(3).apk»** в чате с идентификатором **«3****» 25.01.2026 в 15:28:14**



ЧТО УДАЛОСЬ УСТАНОВИТЬ

- ФАКТ НАЛИЧИЯ ВРЕДОНОСНОГО ПО
- ОТОБРАЖАЕМОЕ НАЗВАНИЕ
- ПОТЕНЦИАЛЬНЫЕ ВОЗМОЖНОСТИ
- СВЯЗЬ СОБЫТИЙ С ДАТАМИ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ



- ВРЕМЯ УСТАНОВКИ И УДАЛЕНИЯ
- SHA-256 ДЛЯ ИДЕНТИФИКАЦИИ
- ИСТОЧНИК ПОЛУЧЕНИЯ APK-ФАЙЛА

СПАСИБО

КОНТАКТЫ:

+7 (495) 909-92-78

support@mko-systems.ru

mko-systems.ru