



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 НЕ РЕДКО 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



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

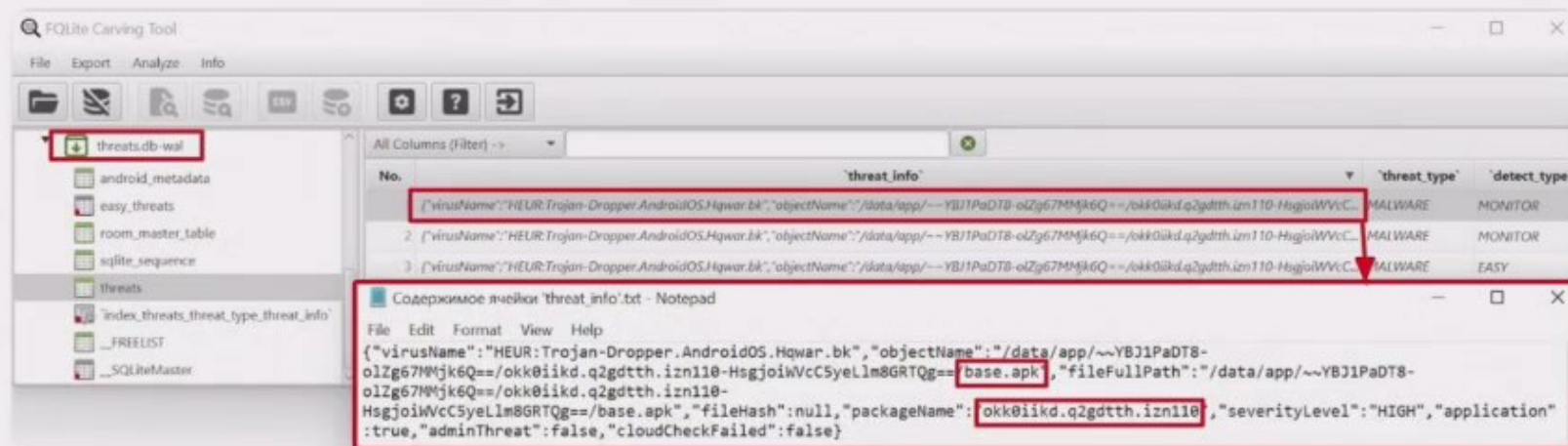
ИНЦИДЕНТ А:

«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.q2gdth.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**

The screenshot shows two windows. The top window is 'palm-a - Notepad' displaying a JSON snippet: `{"currentTime": 1762922355829, "packageName": "okk0iikd.q2gdtth.izn110"},`. The value `1762922355829` is highlighted with a red box. The bottom window is 'DCode v5.5', a time conversion tool. It has a table with 'Name' and 'Timestamp' columns. The first row shows 'Unix Milliseconds (Java Time) (UTC)' with the timestamp '2025-11-12 04:39:15.8290000 Z'. The second row shows 'Unix Milliseconds (Java Time)' with the timestamp '2025-11-12 04:39:15.8290000 +00:00'. To the right, the 'Value Input' section has a 'Format' dropdown set to 'Numeric' and a 'Value' input field containing '1762922355829'. Red arrows indicate the flow of information: one arrow points from the highlighted value in the Notepad window to the 'Value' input field in DCode, and another arrow points from the 'Value' input field to the second row of the timestamp table.

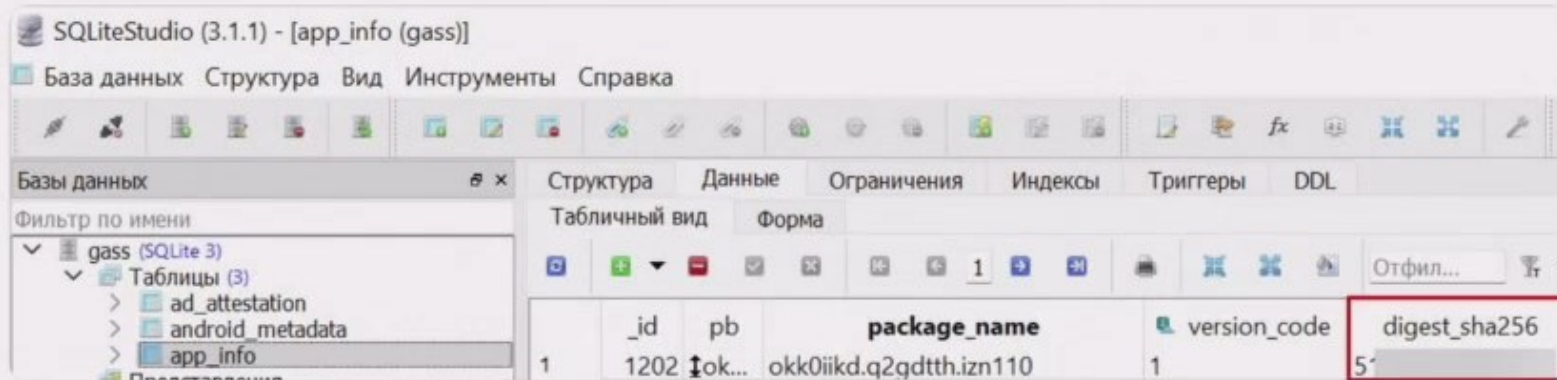
Name	Timestamp
⌚ Unix Milliseconds (Java Time) (UTC)	2025-11-12 04:39:15.8290000 Z
→ ⌚ Unix Milliseconds (Java Time)	2025-11-12 04:39:15.8290000 +00:00

Value Input: Format: Numeric, Value: 1762922355829

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**



SQLiteStudio (3.1.1) - [app_info (gass)]

База данных Структура Вид Инструменты Справка

Базы данных

Фильтр по имени

gass (SQLite 3)

- Таблицы (3)
 - ad_attestation
 - android_metadata
 - app_info

Структура Данные Ограничения Индексы Триггеры DDL

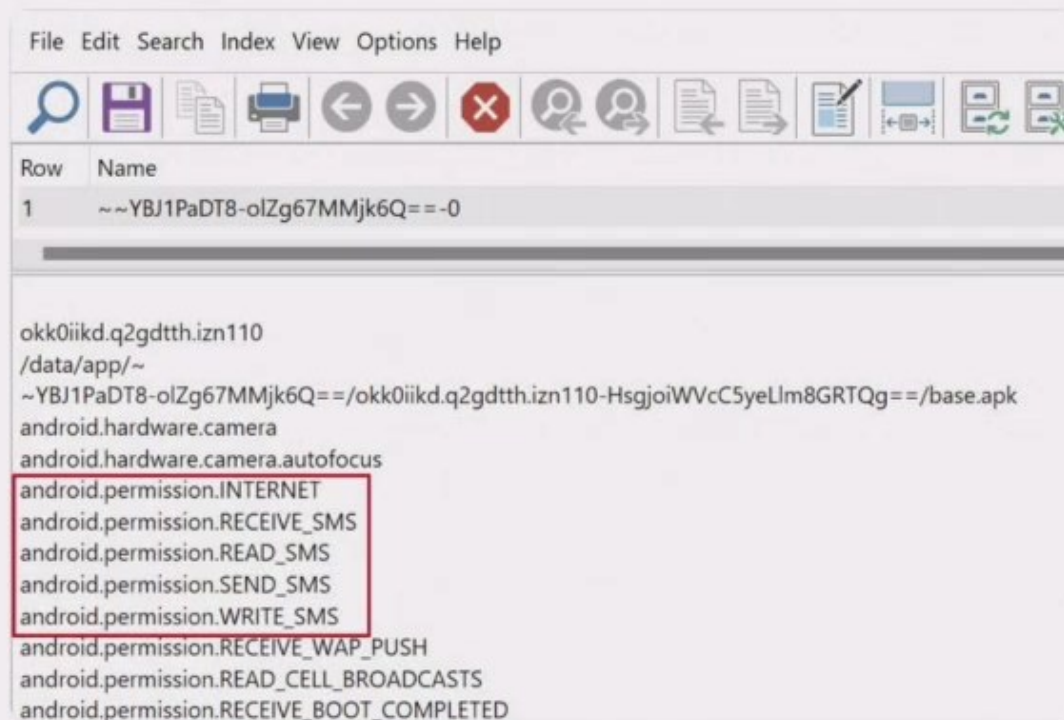
Табличный вид Форма

	_id	pb	package_name	version_code	digest_sha256
1	1202	ok...	okk0iikd.q2gdtth.izn110	1	5

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

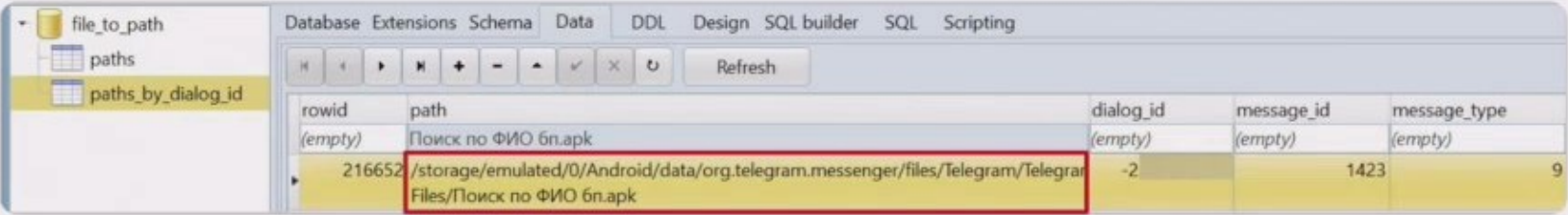
Из файла **PhoneHelper.Db**
установлено, что приложение
с идентификатором
okk0iikd.q2gdtth.izn110
отображалось на устройстве
под именем
«Поиск по ФИО бп»



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

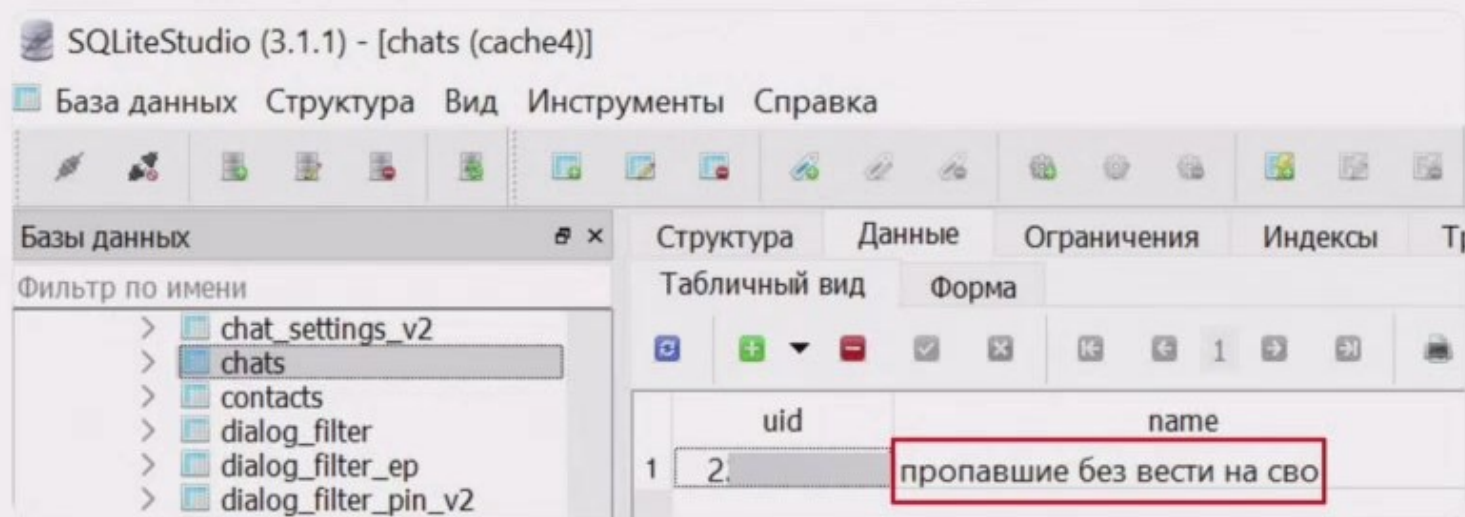


Database Extensions Schema Data DDL Design SQL builder SQL Scripting				
Refresh				
rowid	path	dialog_id	message_id	message_type
(empty)	Поиск по ФИО бп.apk	(empty)	(empty)	(empty)
216652	/storage/emulated/0/Android/data/org.telegram.messenger/files/Telegram/Telegram Files/Поиск по ФИО бп.apk	-2	1423	9

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**»



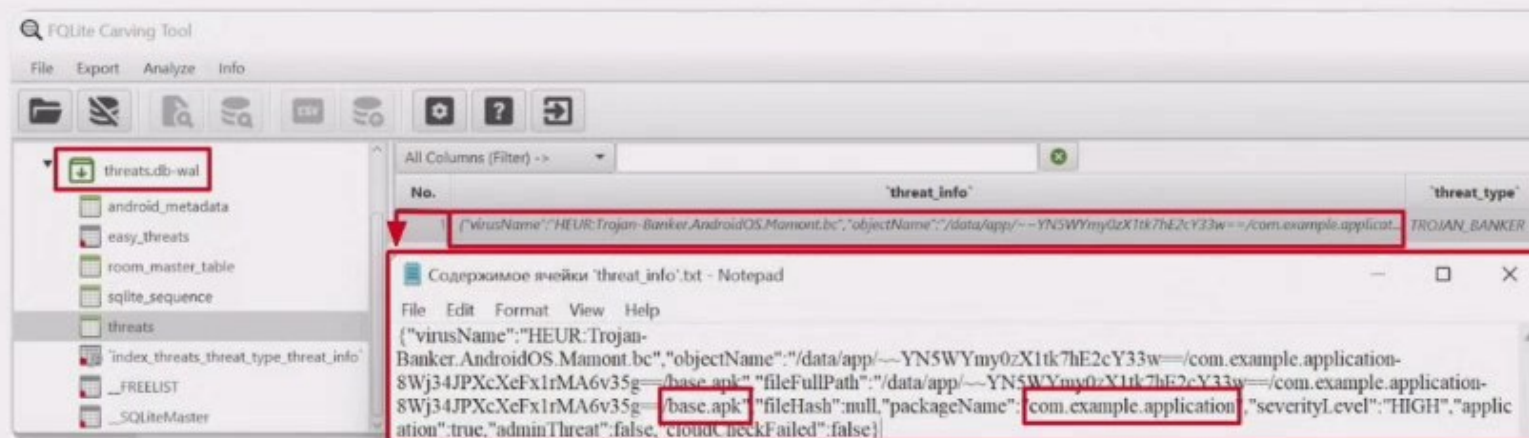
ИНЦИДЕНТ В:

«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 **13.01.2025 в 05:59:20** приложение с идентификатором **com.example.application** было назначено стандартным приложением для работы с SMS

 FileLog1.log - Notepad

File Edit Format View Help

25-01-13 05:59:20.444 ORC/CF(15010): getCOA = 0

25-01-13 05:59:20.452 ORC/CF(15010): getCWA = 0

25-01-13 05:59:20.609 SDK/MCS(15010): cmcEnable = false

25-01-13 05:59:20.786 ORC/DefaultMessageManager(15010): refreshDefaultSmsApp : com.example.application

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



pm_debug_info.txt - Notepad

File Edit Format View Help

```
2025-01-31 17:20:22.528: START DELETE PACKAGE: observer{98976705}  
pkg{com.example.application}, user{0}, caller{10112} flags{2}  
2025-01-31 17:20:29.859: Removing prefs while replacing
```

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

SQLiteStudio (3.1.1) - [app_info (gass)]

База данных Структура Вид Инструменты Справка

Базы данных

Фильтр по имени

gass (SQLite 3)

Таблицы (3)

- ad_attestation
- android_metadata
- app_info

Структура Данные Ограничения Индексы Триггеры DDL

Табличный вид Форма

	_id	pb	package_name	version_code	digest_sha256
1	4152	↑co...	com.example.application	1	0

SQLiteStudio (3.1.1) - [application_rule (adaptivity)]

База данных Структура Вид Инструменты Справка

Базы данных

Фильтр по имени

adaptivity (SQLite 3)

Таблицы (7)

- android_metadata
- application_rule
- history
- room_master_table

Структура Данные Ограничения Индексы

Табличный вид Форма

	packageName	applicationName
1	com.example.application	Photo Archive (20)

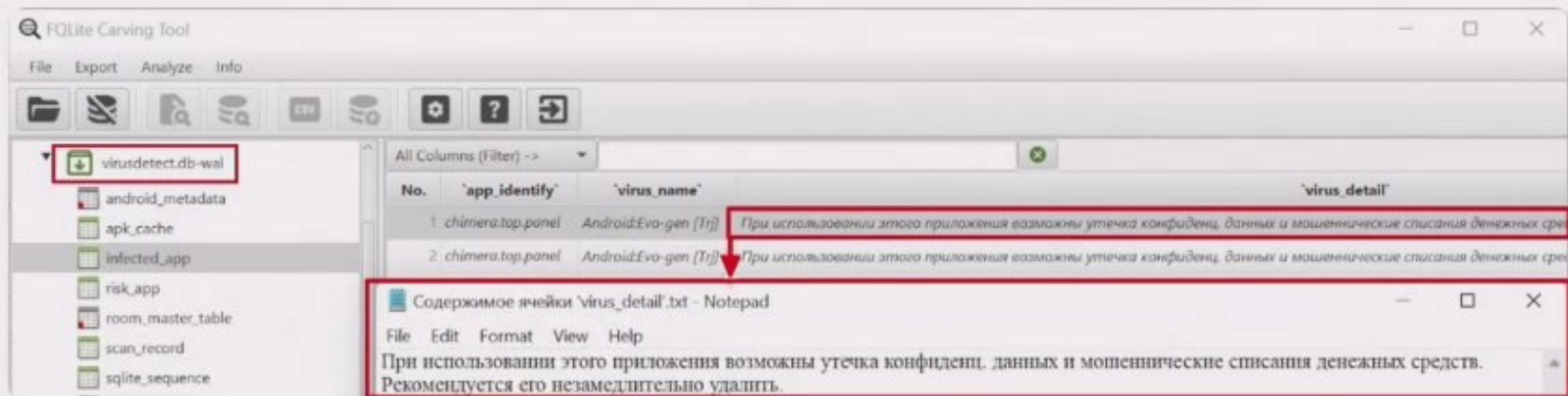
ИНЦИДЕНТ В:

«ВИДЕО.ЧП(З)»

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**

log-1 - Notepad

File Edit Format View Help

25.01.2026 23:56 SessionCommitReceiver Adding package name to install queue. Package name: chimera.top.panel has app icon: false, has app label: false

25.01.2026 23:56 ItemInstallQueue Adding PendingInstallShortcutInfo to queue. Attached info: WorkspaceItemInfo(id=-1 type=APP container=#

com.android.launcher3.logger.Launcher.Atom\$ContainerInfo@7bc6f targetComponent=ComponentInfo {chimera.top.panel/} screen=-1 cell(-1,-1) span(1,1)

minSpan(1,1) rank=0 user=UserHandle{0} title=видео.чп(3)

LogToDump.log - Notepad

File Edit Format View Help

1769609610986 PersistedStoragePackageUninstalledReceiver:d Received android.intent.action.PACKAGE_FULLY_REMOVED for chimera.top.panel for u0

1769610237615

DCode v5.5

File Tools Theme Help

Time Decoding Time Encoding

Name	Timestamp	Value Input
Unix Milliseconds (Java Time)	2026-01-28 14:13:30.9860000 +00:00	
→ Unix Milliseconds (Java Time) (UTC)	2026-01-28 14:13:30.9860000 Z	

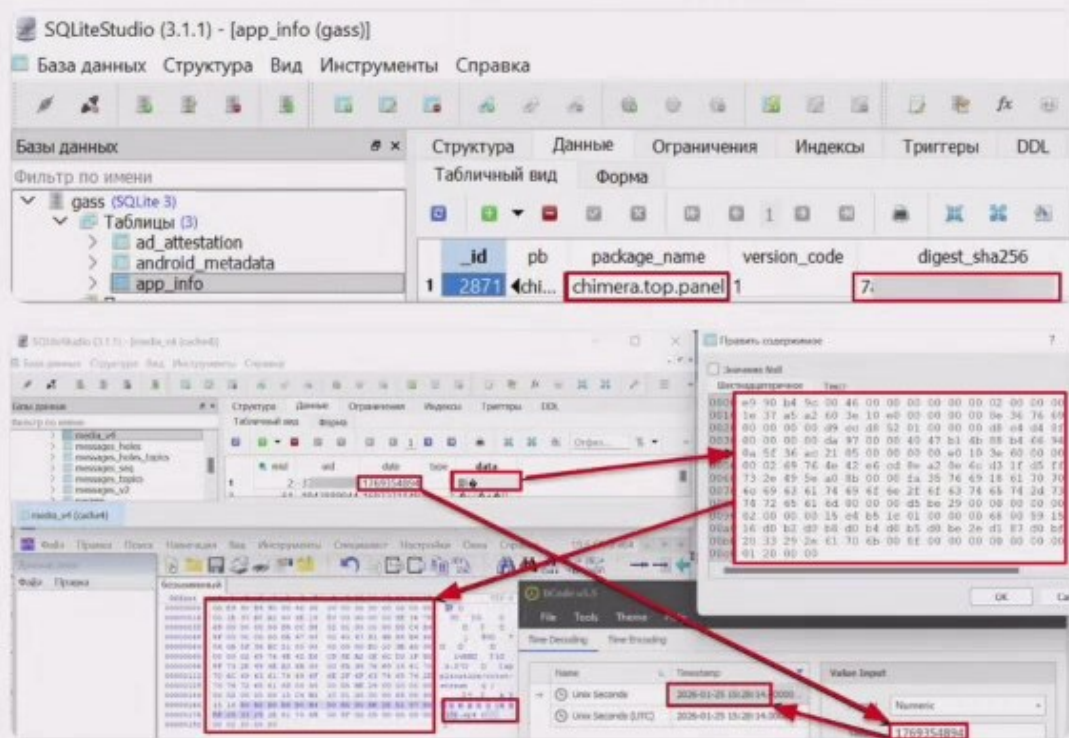
Format Numeric

Value 1769609610986

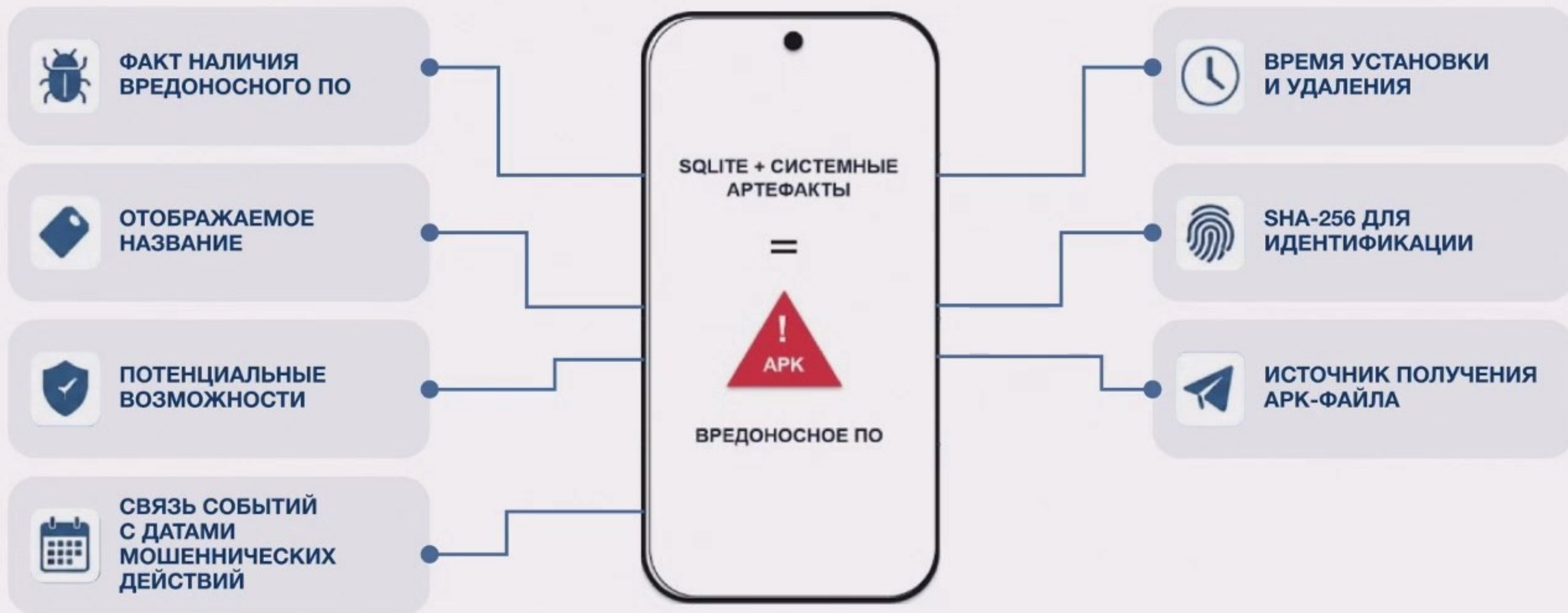
ЦИФРОВОЙ «ОТПЕЧАТОК» И ИСТОЧНИК ПОЛУЧЕНИЯ АРК-ФАЙЛА

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



СПАСИБО

КОНТАКТЫ:

☎ +7 (495) 909-92-78

✉ support@mko-systems.ru

🌐 mko-systems.ru

