MK SYSTEMS

USING SQLITE DATABASE LOGS IN DIGITAL INCIDENT INVESTIGATIONS

THE SQLITE LOG: THE DATABASE'S "BLACK BOX"

1. What databases store
2. Deleted from the database ≠ gone without a trace
3. Real investigation case studies

WHY SQLITE?

A WIDELY USED EMBEDDED DBMS FOR ANDROID, iOS, macOS, WINDOWS AND LINUX

- No separate server required
- Almost no configuration needed
- Stores data in ordinary files
- High performance with a small footprint

WHAT DOES IT STORE?

- Messages
- Location data
- Browser history
- Banking app data
- Contacts
- Settings and service data
- Call logs

SQLITE LOGS OFTEN PRESERVE TRACES OF CHANGES EVEN AFTER DATA IS DELETED FROM THE MAIN DATABASE

1 **MESSAGE**
sent

2 **EDIT**
18:00 → 18:10

3 **DELETION**
record disappears

DATABASE.DB
Final state only

≠

SQLITE LOGS
May retain traces of changes

HOW WAL WORKS:
THE LOG FIRST, THE DATABASE SECOND

APP
Creates, modifies or deletes a record

DATABASE-WAL
Changes are written here first

CHECKPOINT
Transfers changes

DATABASE.DB
Current state

DATABASE.DB
Current data

DATABASE-WAL
Change log

DATABASE-SHM
Service information

WHAT A WAL FILE MAY CONTAIN

New records	Not yet transferred to database.db
Deleted records	Traces of objects no longer in the main database
Previous versions	Earlier states of modified data
Temporary states	Intermediate database states
Incomplete transactions	Events that have not reached a checkpoint

A SIMPLE EXAMPLE: ONE MESSAGE, THREE STATES IN WAL

1 **18:00**
Let’s meet at 18:00

2 **19:00**
Let’s meet at 19:00

3 **DELETE**
Message deleted

THREE INCIDENTS INVOLVING FRAUDULENT LOANS

No.	Victim	Date	Amount	Device	Acquisition method
A	Ivanov I.I.	12.11.2025	11 000	Tecno Spark 8C (Tecno KG5n)	Unisoc / Spreadtrum Android
B	Petrov P.P.	13.01.2025	34 000	Samsung Galaxy M12 (SM-M127F)	Full file system
C	Sidorov S.S.	25.01.2026	23 000	Realme Note 50 (RMX3834)	Unisoc / Spreadtrum Android

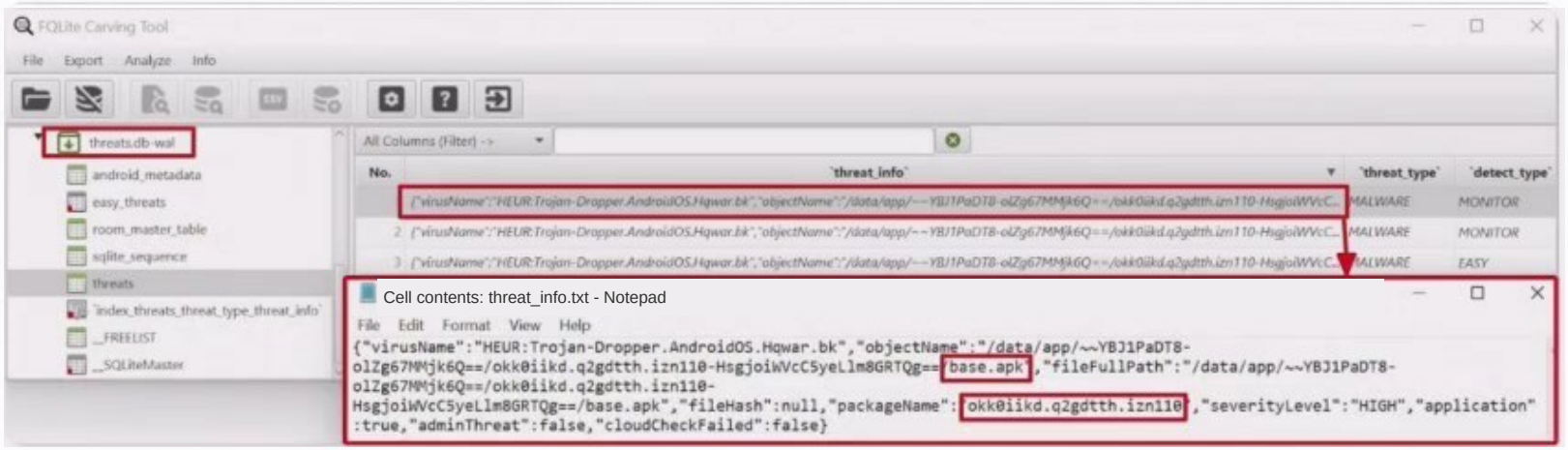
INCIDENT A:

“SEARCH BY FULL NAME BP”

TRACES OF MALWARE

INCIDENT A

The SberBank Online **threats.db-wal** log contained a record for **base.apk**, detected by the built-in antivirus as **HEUR:Trojan-Dropper.AndroidOS.Hqwar.bk.** The file was already absent, but its identifier survived: **okk0iikd.q2gdtth.izn110**

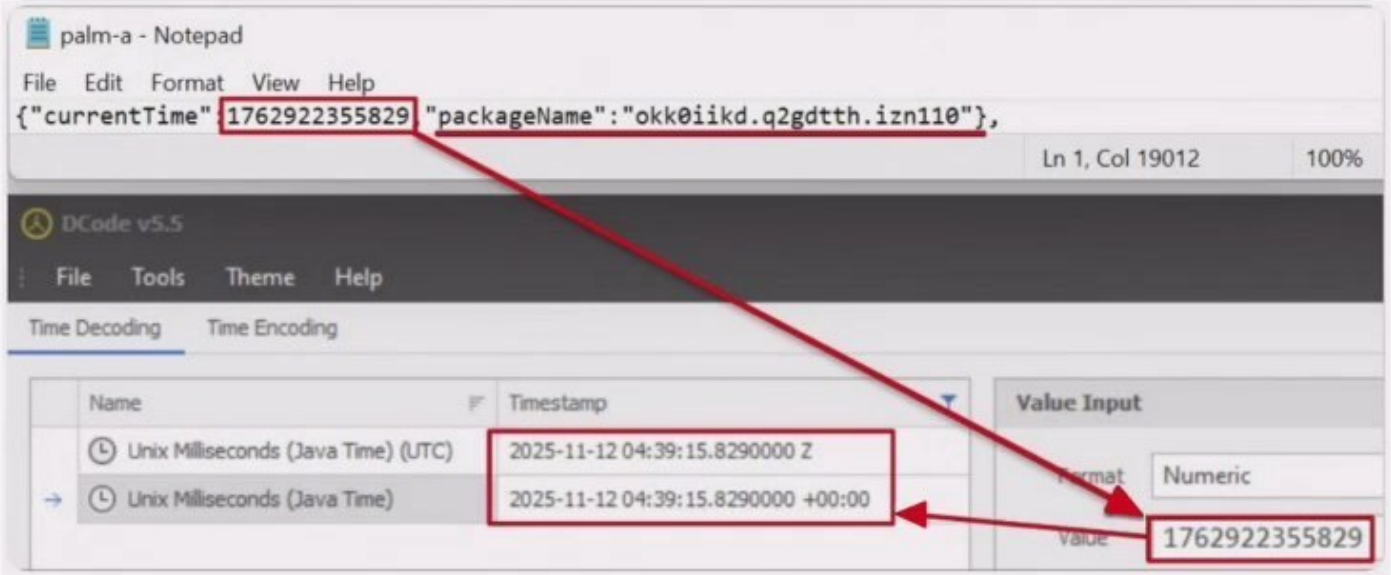


CONFIRMING APP INSTALLATION

INCIDENT A

No record of **okk0iikd.q2gdtth.izn110** was found in **packages.xml**.

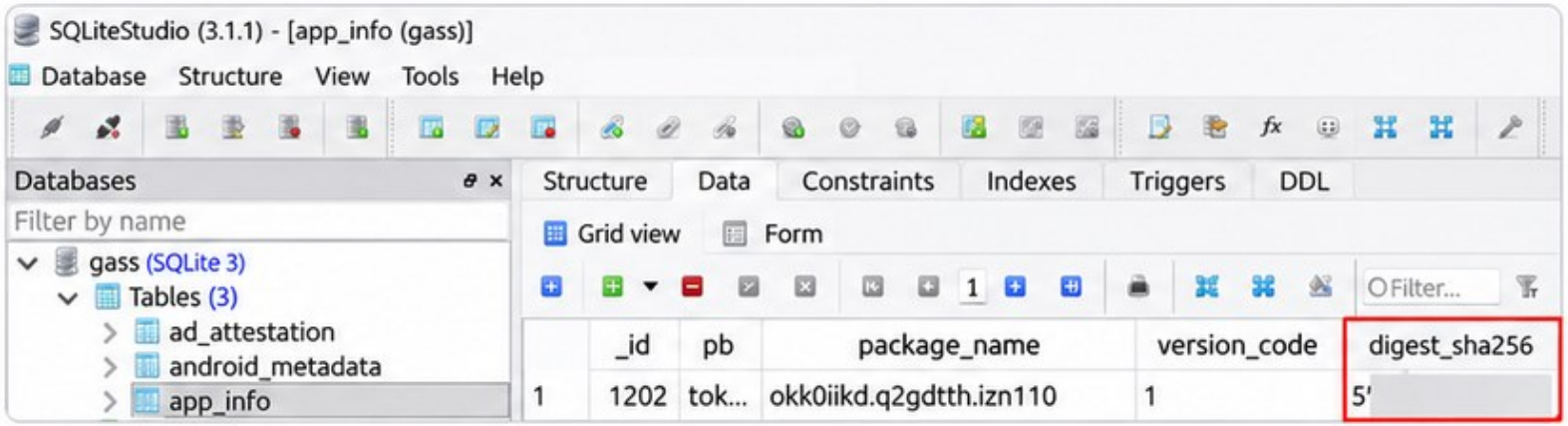
However, the **palm-a** service log retained its registration event on **12.11.2025** at **04:39:15**.



RECOVERING A DIGITAL FINGERPRINT

INCIDENT A

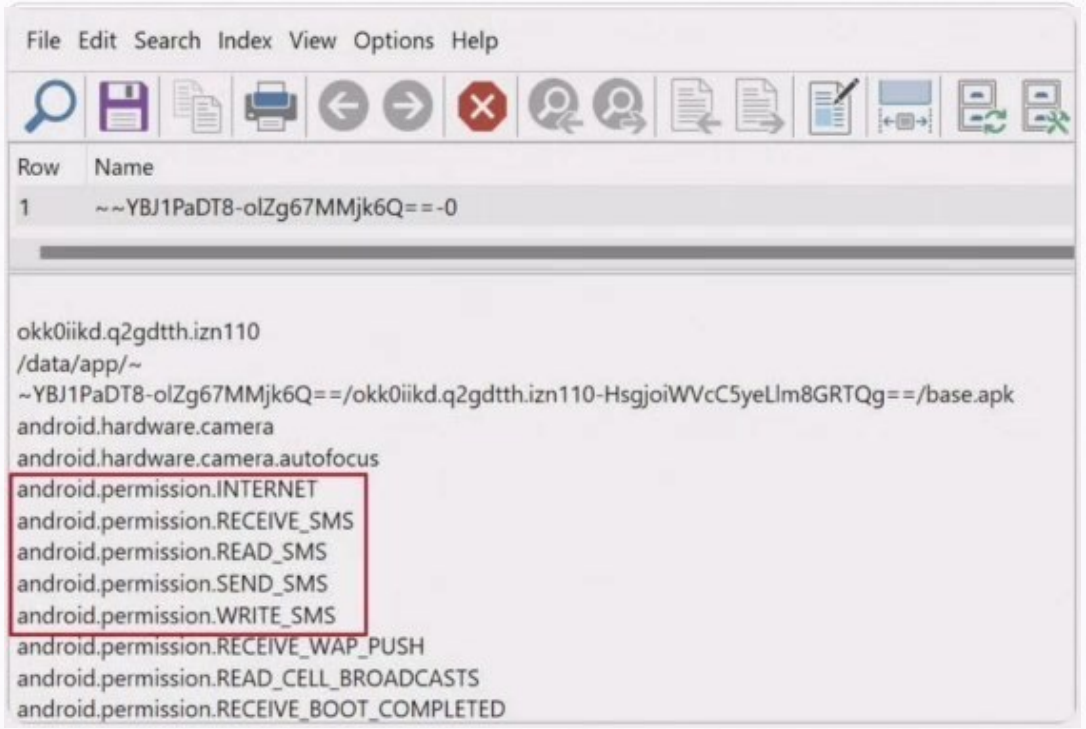
The **gass.db** system database retained the **SHA-256** checksum of the installation file for the app with **identifier okk0iikd.q2gdtth.izn110.**



APP CAPABILITIES

INCIDENT A

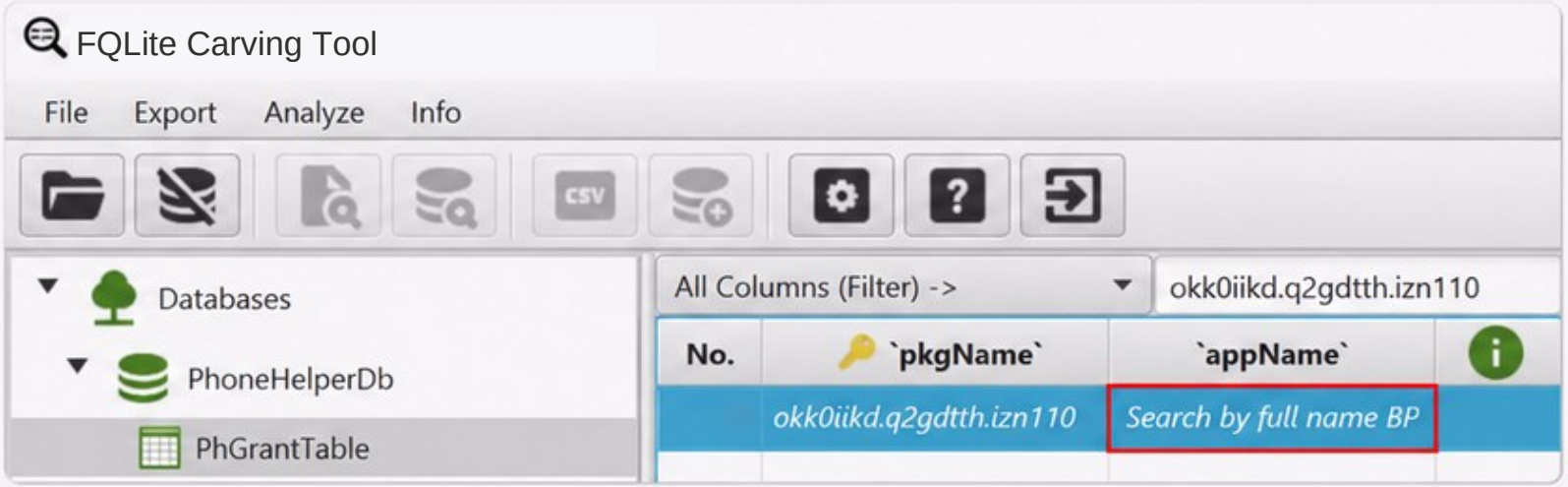
AndroidManifest.xml contained the permissions requested from Android by the app **okk0iikd.q2gdtth.izn110**: **Internet access and receiving and sending SMS messages.**



APP DISPLAY NAME

INCIDENT A

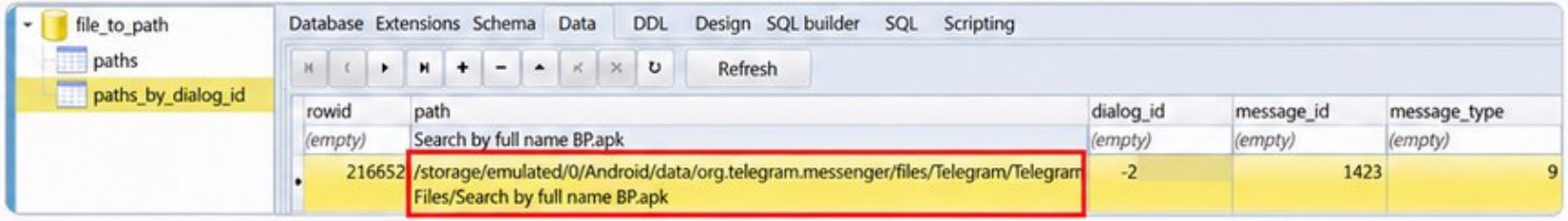
PhoneHelper.Db established that the app **okk0iikd.q2gdtth.izn110** was displayed on the device as **“Search by full name BP”**.



HOW THE APP REACHED THE DEVICE

INCIDENT A

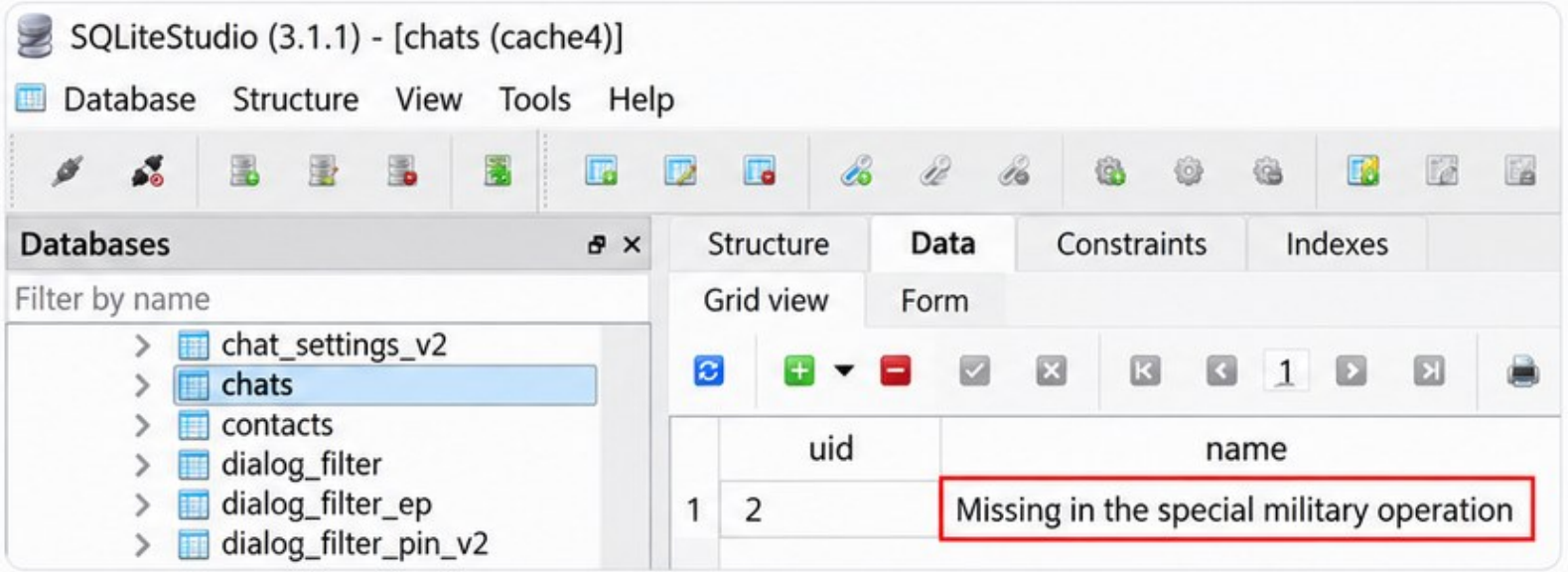
Telegram's file_to_path.db database contained a record showing that **"Search by full name BP.apk"** had been received in a chat.



WHAT THE TELEGRAM CHAT REVEALED

INCIDENT A

The Telegram **messages_v2** table contained no messages. However, the **chats** table retained the chat name: **“Missing in the special military operation”.**



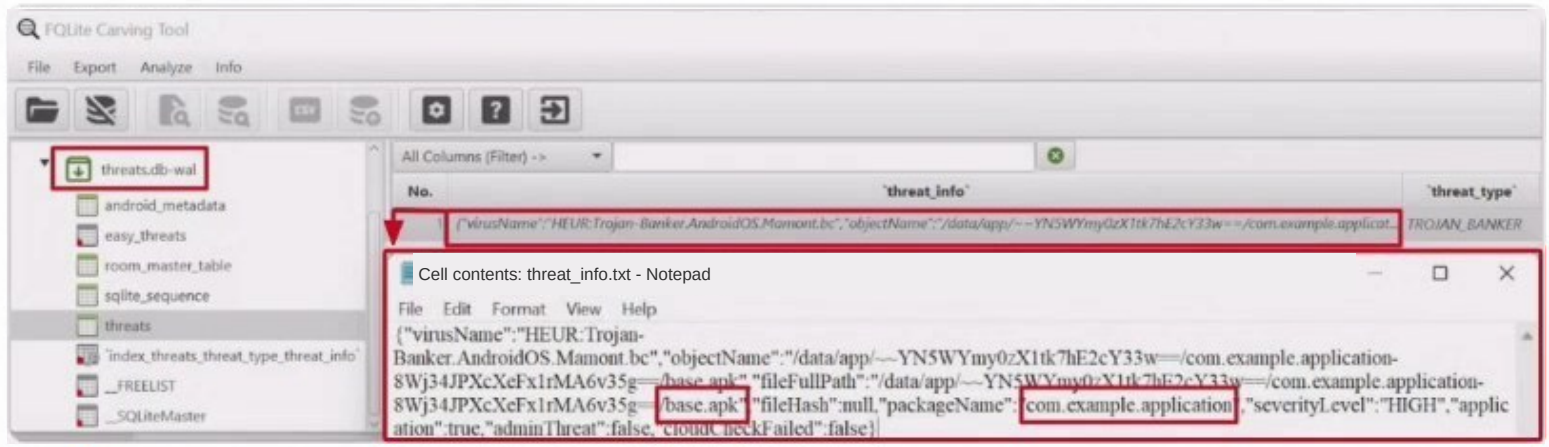
INCIDENT B:

“PHOTO ARCHIVE (20)”

TRACES OF MALWARE

INCIDENT B

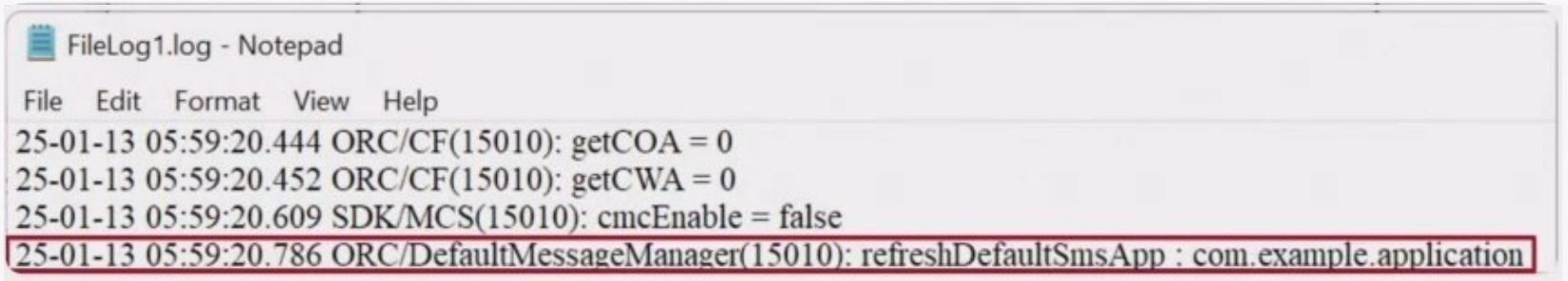
The SberBank Online **threats.db-wal** log retained a record for **base.apk**, detected by the built-in antivirus as **HEUR:Trojan-Banker.AndroidOS.Mamont.bc.** The file was absent, but the log retained its identifier: **com.example.application**



APP CAPABILITIES

INCIDENT B

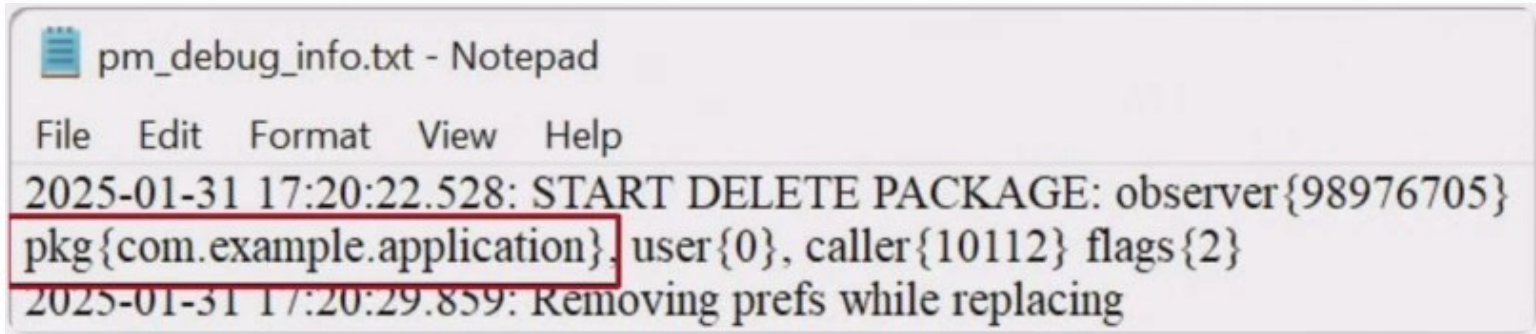
Analysis of **FileLog1.log** confirmed that on **13.01.2025** at **05:59:20**, the app com.example.application was set as the default SMS application.



CONFIRMING APP REMOVAL

INCIDENT B

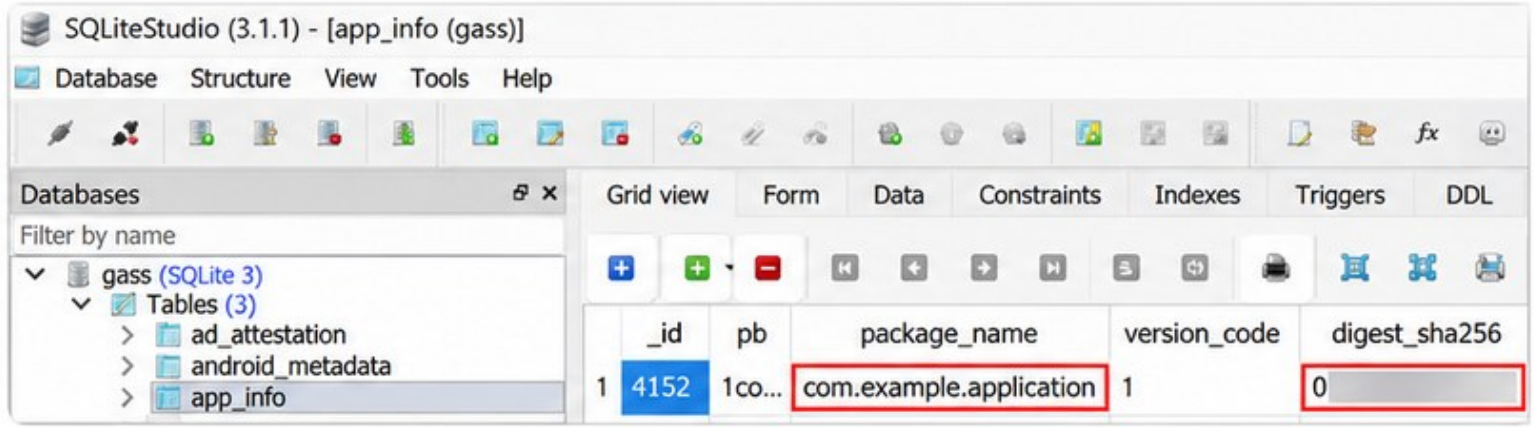
Analysis of **pm_debug_info.txt** confirmed that **com.example.application** was removed on **31.01.2025 at 17:20:22.**

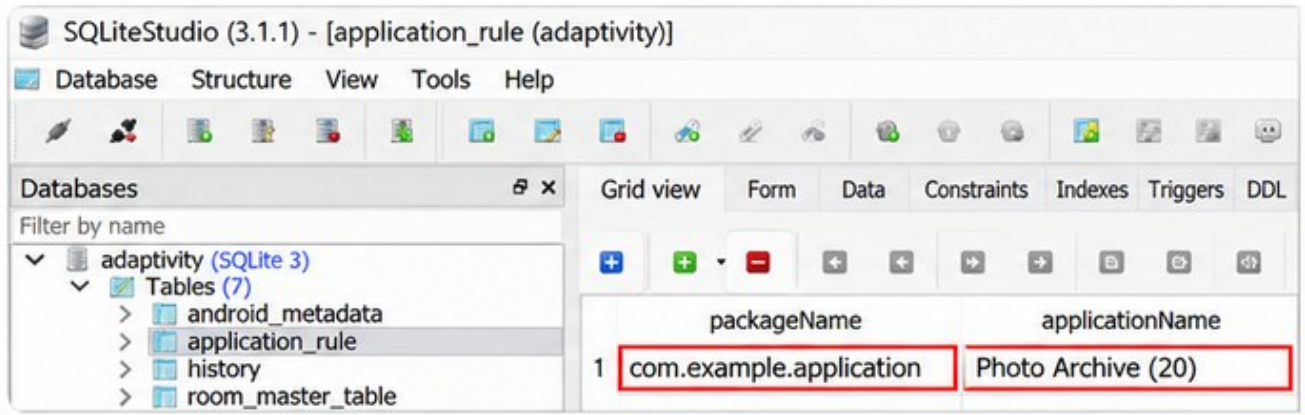


DIGITAL FINGERPRINT AND APP NAME SOURCE OF THE APK FILE

INCIDENT B

- The **gass.db** system database retained the SHA-256 checksum of the installation file for **com.example.application**.
- The antivirus service database **adaptivity.db** retained the app display name: **“Photo Archive (20)”**.
- Telegram’s **cache4.db** contained a record of **“Photo Archive (20).apk”** being received in a chat.





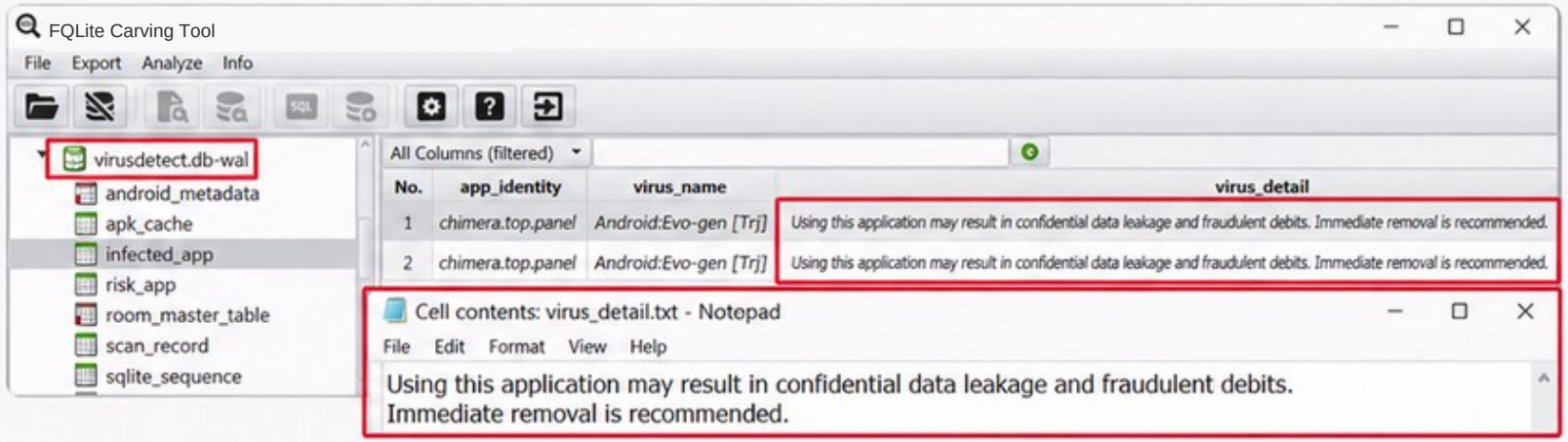
INCIDENT C:

“VIDEO.INCIDENT(3)”

TRACES OF MALWARE

INCIDENT C

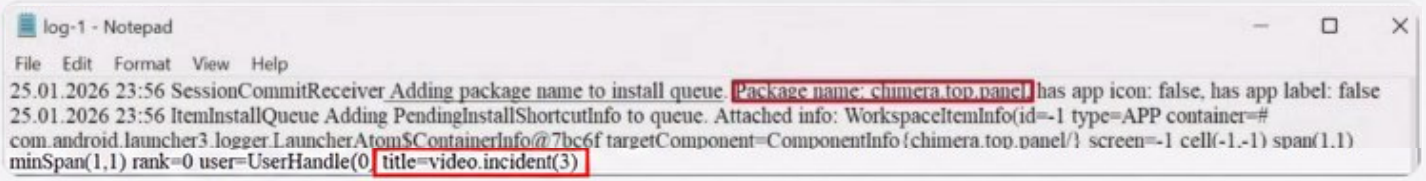
The **virusdetect.db-wal** log contained a record for **chimera.top.panel**, classified by the built-in antivirus as **Android:Evo-gen [Trj]**. The log also warned of possible confidential data leakage and fraudulent debits.

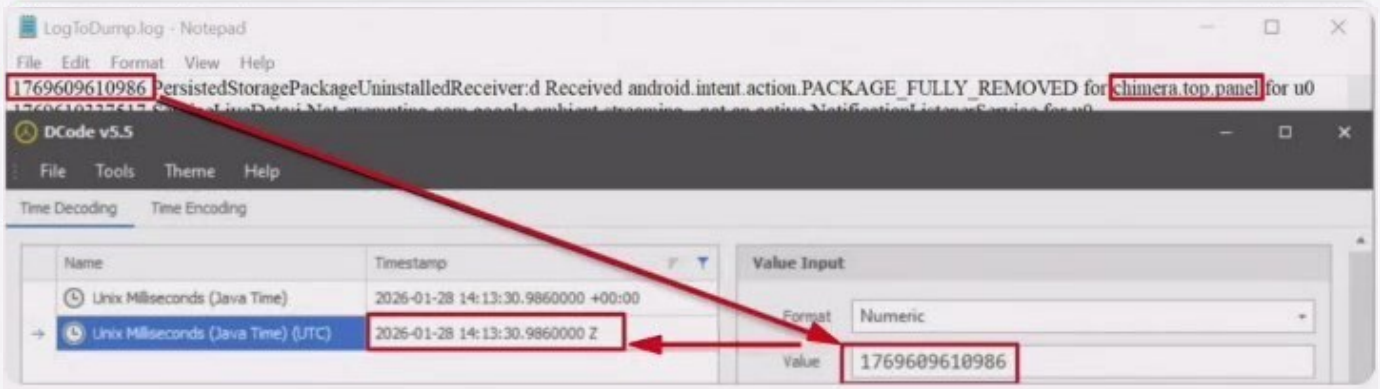


CONFIRMING APP INSTALLATION AND REMOVAL

INCIDENT C

- The log-1 file recorded installation of **chimera.top.panel** on **25.01.2026 at 23:56** and its display name, “video.incident(3)”.
- **LogToDump.log** confirmed removal of the app on **28.01.2026 at 14:13:30.**



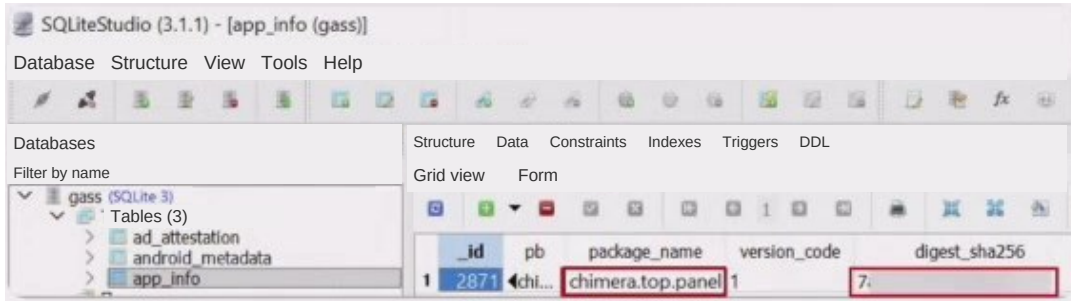


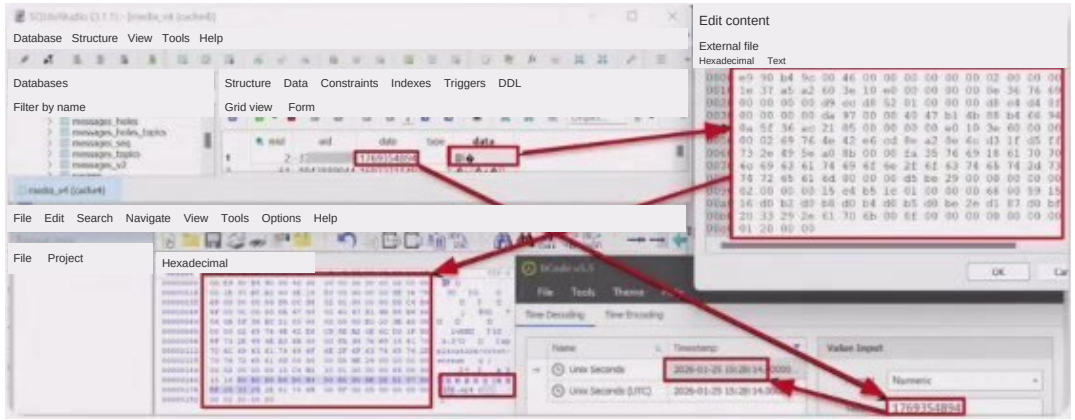
DIGITAL FINGERPRINT AND SOURCE OF THE APK FILE

INCIDENT C

- The **gass.db** system database retained the SHA-256 checksum of the installation file for **chimera.top.panel.**

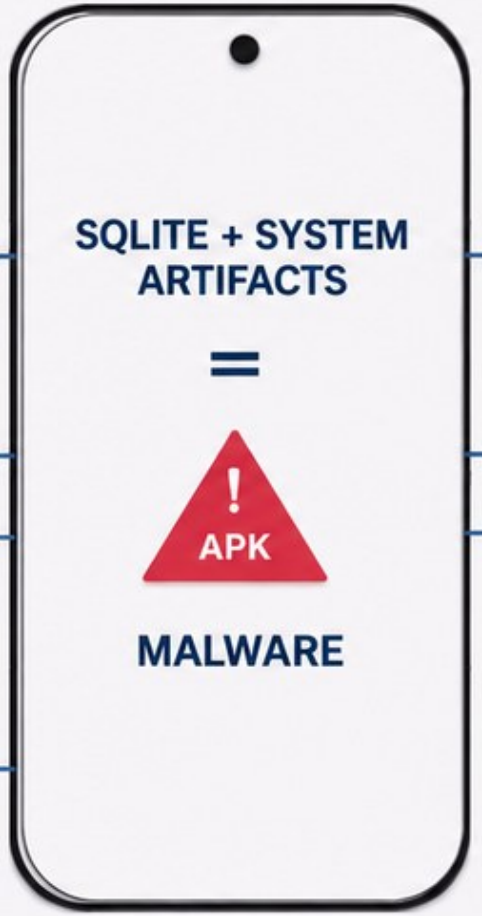
- Telegram's **cache4.db** recorded receipt of **"video.incident(3).apk"** in the chat identified as **"3****"** on **25.01.2026 at 15:28:14.**





WHAT THE INVESTIGATION ESTABLISHED

- PRESENCE OF MALWARE
- APP DISPLAY NAME
- POTENTIAL CAPABILITIES
- LINKS BETWEEN EVENTS AND DATES OF FRAUD



- INSTALLATION AND REMOVAL TIMES
- SHA-256 FOR IDENTIFICATION
- SOURCE OF THE APK FILE

THANK YOU

CONTACTS:

+7 (495) 909-92-78

support@mko-systems.ru

mko-systems.ru