

Evaluating Cellebrite UFED and Physical Analyzer against WhatsApp, Signal and Telegram on Android 16

Smit Brijeshkumar Patel

Student ID 2506590 · MSc Cybersecurity and Digital Forensics

Supervisor: Dr Ramzi Djemai · UWTSD London

390

seeded items

4

extraction attempts

0

items recovered

Evidence is on the phone. Testing stopped short.

The problem



Encryption pushed evidence onto the phone

WhatsApp and Signal encrypt messages end to end by default, so intercepted traffic no longer gives you the content [1], [2].



Examiners lean on commercial tools

Tools like Cellebrite get to that data, and most claims about what they can do come from the vendor [3].



Silence is the risk

When a tool returns no messages, nothing independent tells the examiner whether they were missing or never reached.

NIST CFTT, latest Cellebrite cycle [4]

The only independent test of the platform

WhatsApp

Account details only

Signal

Not tested

Telegram

Not tested

Message content

Never checked

How much does Cellebrite actually get back?

Aim, objectives and research questions

Aim Measure how much of WhatsApp, Signal and Telegram UFED and Physical Analyzer recover from an Android 16 phone, and work out what follows when the tool does less than it claims.

01

Review

What has been tested, and how each app stores and protects its data

RQ1 How do the apps store and protect data on Android 16, and what has testing established?

02

Design and execute

Controlled extraction on identical seeded data, all three apps

RQ2 How much of a known corpus is recovered, per app and per method?

03

Measure

Completeness, accuracy, media integrity, acquisition time

RQ3 What are the admissibility and custody consequences when a method fails?

04

Assess and produce

Legal impact under Directive (EU) 2016/680; practitioner framework

Nobody had tested all of it at once

Literature and gap

Study	Uses Cellebrite	Tests message content	All three apps	Unrooted device, file system route
NIST CFTT [4], [5]	Yes	No	No	Categories only
Heath et al. 2023 [6]	Yes	Yes	No (WA, Telegram)	No (logical only)
Vasilaras et al. 2022 [7]	Yes (PA 7.50)	Yes	No (Telegram)	No (rooted, Android 9/11)
Sinaga et al. 2026 [8]	Yes	No (artefact counts)	No	No (logical only)
Riadi et al. 2022 [9]	No	Yes	No (Signal)	—
This study	Yes (UFED 7.76)	Yes	Yes	Attempted, Android 16

The gap: no one had tested UFED and Physical Analyzer against all three apps on current Android, through the file system route, with the scoring set before extraction.

A phone where I knew every message

Methodology

Research design (Saunders) [10]

Philosophy	Positivist
Approach	Deductive
Strategy	Design Science Research [11] + experiment
Choice	Quantitative
Time horizon	Cross-sectional
Procedure	NIST SP 800-101r1 phases [12]



Test setup

- Samsung Galaxy S25 Ultra (SM-S938B)
- Android 16, One UI 8.5, unrooted throughout
- UFED 4PC 7.76.0.24 (Educational licence)
- Physical Analyzer 7.73.0.11
- WhatsApp 2.26.35.75, Signal 8.26.4, Telegram 12.10.1 (cloud chats)

390

seeded items, 130 per app: 100 messages + 30 media (10 photos, 10 videos, 10 audio)

42

deleted items (14 per app), a subset of the 390

WA-S-001

Each message body starts with a token. I hashed the media before sending and logged everything.

The same error, four times over

Acquisition attempts

A1 File System (Android Backup) c. 10 min Backup error	A2 File System (Android Backup) c. 39 min Backup error	A3 Advanced Logical (all content types) 29 min Partial	A4 Advanced Logical (after firmware update) 47 min Partial
16 Sep	16 Sep	16 Sep	22 Sep

Every attempt: "ADB backup failed. Shared memory was partially extracted or failed"

In A3 and A4 it came up during the Files stage. UFED kept going and marked both **completed successfully (Figures 1, 2)**.

What the screens showed

Evidence from the extraction (identifiers redacted)

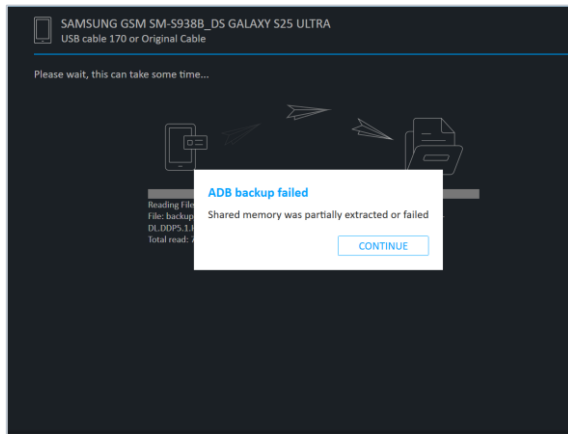


Figure 1: A1, File System (Android Backup). UFED stops with "ADB backup failed", 16/09/2026.

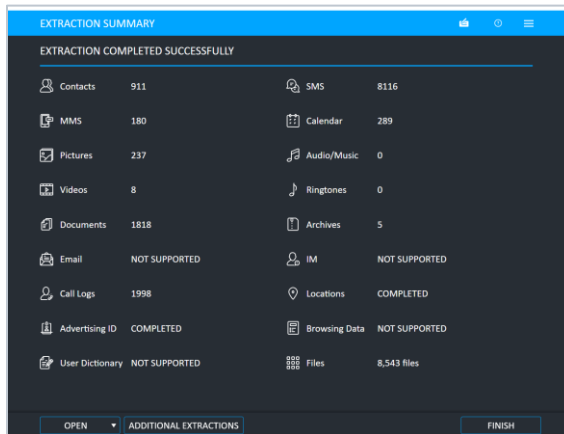


Figure 2: A4, Advanced Logical. Summary reads "completed successfully"; IM shows "not supported", 22/09/2026.

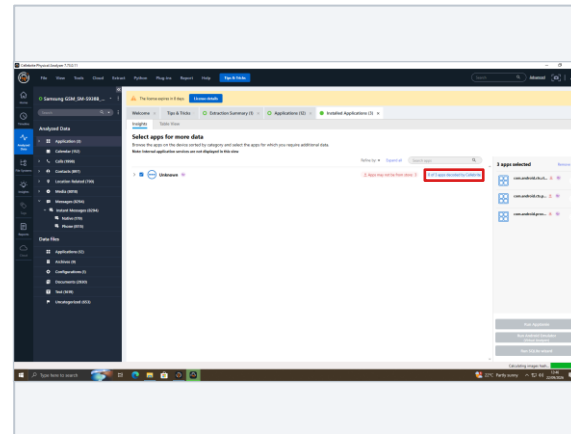


Figure 3: A4 in Physical Analyzer. Three Android system packages, "0 of 3 apps decoded"; no messaging app listed.

The status screen reported success. The decoder found no messaging app to work on.

All 390 items: not acquired

Results

0 / 390

items recovered. Completeness is 0% for every app and method. With nothing recovered, accuracy and media integrity can't be measured.

A4 still held plenty of system data:

8,116

SMS

911

contacts

8,543

files

Five-state recovery rubric

Fully recovered 0

Partially recovered 0

Present but undecoded 0

Absent 0

Not acquired 390

Physical Analyzer: reported "0 of 3 apps decoded" (Figure 3) and did not list the messengers. A search for the corpus tokens came back empty.

Four barriers, and any one would do it

Why the ladder stopped



adb backup excludes modern apps

Since Android 12, apps targeting API 31+ are left out of adb backup [13]. Google Play requires far higher targets [14].



Apps can opt out

android:allowBackup="false" excludes an app from backup [15]; WhatsApp is reported to set it [16].



File-based encryption + Knox

App storage stays credential-encrypted; Samsung binds keys in TrustZone and Knox Vault [17], [18].



Signal encrypts its own database

SQLCipher with the key in the Android Keystore: a copied file is still ciphertext [19].

Troubleshooting (Auto Blocker off, File Transfer mode, Stay Awake, new port and cable, antivirus paused, restarts) **only ever touched the connection. The block was in Android and the apps, as Cellebrite's own guidance says [20].**

The tool said success. The app data never came.

Legal and evidential implications



Admissibility

- Hashes and screenshots cover integrity
- Completeness fails, and the tool gave no warning
- ENFSI expects that uncertainty to be declared [21]



Chain of custody

- A1 and A2 still count as actions on the exhibit
- Firmware updated between A3 and A4
- A3 and A4 hashes differ, which is normal for a live phone [22]



Directive (EU) 2016/680

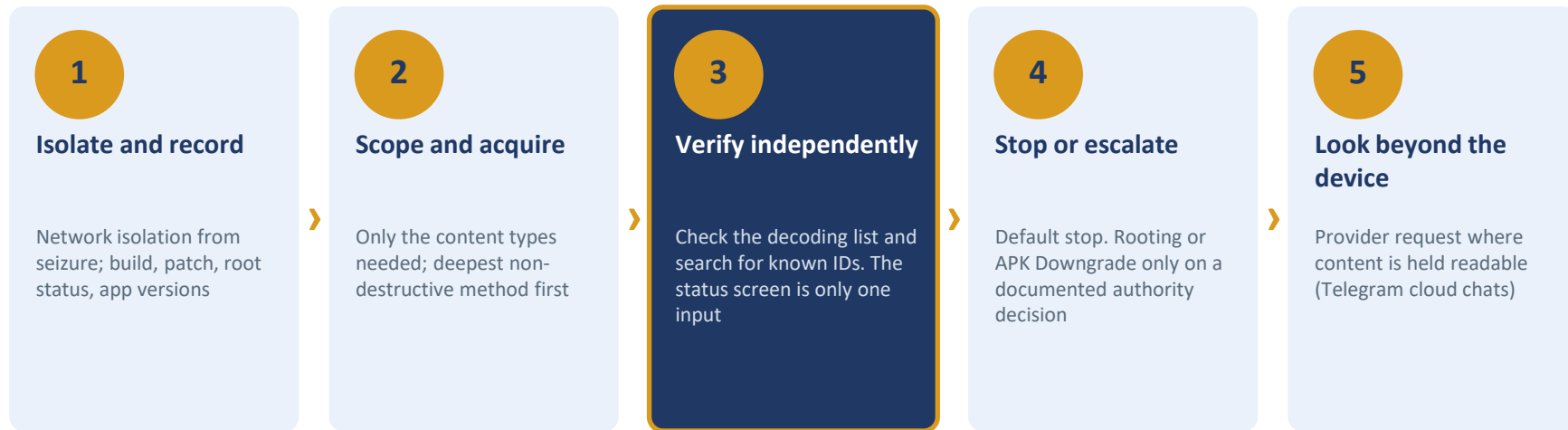
- Art. 4: record "not acquired", never "empty"
- Art. 6: third-party contacts and SMS swept up
- Art. 25: failed attempts belong in the log



Telegram is different off the phone. Its cloud chats sit readable on its servers, so a European Production Order (Reg. (EU) 2023/1543) could return them [23], [24]. WhatsApp and Signal hold no readable copy.

Five steps for when the tool comes back empty

The artefact



A checklist adds eleven fields to log at every attempt, such as the exact error text and the tool's status next to the checked status. Each one traces back to a failure in this experiment.

What I did, and the proof

Demonstration



1. Seeded the phone

390 items across three apps, each message tokenized and each media file hashed; 42 deleted. Ground truth log records it all



2. Ran four extractions

A1, A2 File System (Android Backup); A3, A4 Advanced Logical, six days apart



3. Read UFED's own output

Backup error every time; A4 still "completed successfully" (Figures 1, 2)



4. Decoded in Physical Analyzer

"0 of 3 apps decoded", no messenger listed, token search empty (Figure 3)



5. Kept every hash

UFED hashed each archive and report at acquisition; A4 report: 337FE871...9375515F (appendix)

A real limit, written down properly

Conclusion

Contribution

- A dated, repeatable limit: UFED 7.76 on an unrooted Android 16 S25 Ultra recovered nothing from the three apps
- A "not acquired" state that separates unreached from missing
- Evidence that a tool's success status cannot be taken at its word
- A practitioner framework built on those failures

Limitations

- One handset, one tool version, Educational licence
- Firmware update between sessions
- Notification logs not examined
- Framework not yet tested by practitioners

Future work

- Higher licence tier, XRY and AXIOM on the same model
- Rooted twin handset to measure app-level differences
- OS sources such as notification logs
- Framework trials in casework

Appendix: hash values recorded by UFED at acquisition

Appendix

Attempt	Date	File	SHA-256
A3	16/09/2026	Extraction archive (.zip)	A853A2D9D3E9BC4E83E721E16E6EF53B012BE6F0087DFB31B3651B5AFB1B1D70
A3	16/09/2026	SummaryReport.pdf	EF784ACEEF61B8F6C35DA7A98594ACAF8BAF4B9D484AB4959619E5246A461DE
A4	22/09/2026	Extraction archive (.zip)	EF0083D0CA866DE3D6D00C7CDAC51094A0F212DA41836B091E5B3E98435FBF3E
A4	22/09/2026	SummaryReport.pdf	337FE871774A351D02195433860E11D69D0AC82CBFED699900C7D9D79375515F

A3 and A4 hashes differ because a live phone keeps writing between extractions [22].

References (1 of 2)

References

- [1] A. R. Onik, J. Brown, C. Walker, and I. Baggili, "A systematic literature review of secure instant messaging applications from a digital forensics perspective," *ACM Computing Surveys*, vol. 57, no. 9, art. 239, 2025.
- [2] WhatsApp LLC, "WhatsApp encryption overview: Technical white paper," 2025. [Online]. Available: [whatsapp.com/security](https://www.whatsapp.com/security)
- [3] B. Fakiha, "Unlocking digital evidence: Recent challenges and strategies in mobile device forensic analysis," *J. Internet Services and Information Security*, vol. 14, no. 2, pp. 68-84, 2024.
- [4] NIST, "Test results for mobile device acquisition tool: Cellebrite Inseyets.UFED v10.3.0.260 - Inseyets.PA v10.3.0.3169," DHS Science and Technology Directorate, 2024.
- [5] NIST, "Test results for mobile device acquisition tool: UFED4PC v7.60.0.222 - Physical Analyzer v7.58.0.66," DHS Science and Technology Directorate, Feb. 2023.
- [6] H. Heath, A. MacDermott, and A. Akinbi, "Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data?," *Forensic Sci. Int.: Digital Investigation*, vol. 46, art. 301585, 2023.
- [7] A. Vasilaras, D. Dosis, M. Kotsis, and P. Rizomiliotis, "Retrieving deleted records from Telegram," *Forensic Sci. Int.: Digital Investigation*, vol. 43, art. 301447, 2022.
- [8] S. J. Sinaga et al., "Comparative evaluation of artifact extraction performance and usability in digital forensic tools: A study of Cellebrite UFED, MSAB XRY, and Magnet AXIOM," *J. Forensic Sciences*, 2026, doi: 10.1111/1556-4029.70320.
- [9] I. Riadi, Herman, and N. H. Siregar, "Mobile forensic analysis of Signal messenger application on Android using DFRWS framework," *Ingenierie des Systemes d'Information*, vol. 27, no. 6, pp. 903-913, 2022.
- [10] M. N. K. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*, 9th ed. Harlow, U.K.: Pearson, 2023.
- [11] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75-105, 2004.

References (2 of 2)

References

- [12] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on mobile device forensics," NIST SP 800-101 Rev. 1, 2014.
- [13] Android Developers, "Behavior changes: Apps targeting Android 12," Google. [Online]. Available: developer.android.com
- [14] Google, "Target API level requirements for Google Play apps," Play Console Help. [Online]. Available: support.google.com
- [15] Android Developers, "Back up user data with Auto Backup," Google. [Online]. Available: developer.android.com
- [16] Privacy International, "A technical look at phone extraction," Oct. 2019. [Online]. Available: privacyinternational.org
- [17] Android Open-Source Project, "File-based encryption," Android Documentation. [Online]. Available: source.android.com
- [18] Samsung, "Data protection," Samsung Knox Mobile Security White Paper. [Online]. Available: docs.samsungknox.com
- [19] J. Son, Y. W. Kim, D. B. Oh, and K. Kim, "Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema," Forensic Sci. Int.: Digital Investigation, vol. 40, art. 301347, 2022.
- [20] P. Lorentz and H. Mahalik, "Android data collection simplified," Cellebrite, Jul. 2020. [Online]. Available: cellebrite.com
- [21] ENFSI, "Best practice manual for the forensic examination of digital technology," ENFSI-BPM-FIT-01, ver. 01, Nov. 2015.
- [22] S. Yoo, Y. Park, and D. Jeong, "Preserving evidence integrity in full file system extractions: Assessing hash inconsistencies and potential solutions," J. Forensic Sciences, vol. 71, no. 5, pp. 2070-2087, 2026.
- [23] Telegram, "MTProto mobile protocol," Telegram API Documentation. [Online]. Available: core.telegram.org/mtproto
- [24] European Parliament and Council, "Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings," OJ L 191, pp. 118-180, 2023.

Thank you

Questions?

Smit Brijeshkumar Patel

Student ID 2506590 · MSc Cybersecurity and Digital Forensics

Supervisor: Dr Ramzi Djemai · UWTSD London