



MSc CYBERSECURITY & DIGITAL FORENSICS | ACFA7003 MASTER'S PROJECT

Mobile Device Forensics on Modern Android Devices

A controlled comparison of Cellebrite UFED and Autopsy for recovering deleted messages, media and app data

Vaishnavi Riteshkumar Patel | Enrolment 2503493
University of Wales Trinity Saint David | September 2026

Why Deleted Data on Android Is Hard

A phone now holds a person's messages, locations, payments and photos in one encrypted volume. Deleted messages are often the evidence that decides a case, and also the evidence most open to challenge.

When a tool finds nothing, the examiner cannot tell whether the data was destroyed by the platform or missed by the software.



File-based encryption

Device state at seizure decides whether app data is readable at all.



Verified boot & hardware keys

Block the modifications that once made physical imaging routine.



Scoped storage

Changes where apps are allowed to write their media.



TRIM & flash controllers

Deleted blocks can be erased before anyone reaches the device.

The Research Gap



What earlier studies did

- Compared tools against each other (Mehta et al., Farnan et al., Wangchuk et al.)
- Used the stronger tool as the reference, so items both tools missed stayed invisible
- Reported no precision figures, because false positives need an independent record



What this study set out to do

- Fix a hashed ground truth before anything is deleted
- Score a commercial and an open-source chain against the same manifest
- Report recovery and precision, on current Android hardware

Aim and Research Questions

AIM Evaluate, under controlled and repeatable conditions, how much deleted data can be recovered from current Android devices, comparing a commercial suite with an open-source workflow against a ground-truth dataset.

RQ1

Which classes of deleted data remain recoverable, and in what proportion?

RQ2

How does acquisition method affect volume and fidelity?

RQ3

How do the two chains compare on recovery, precision, metadata, integrity and time?

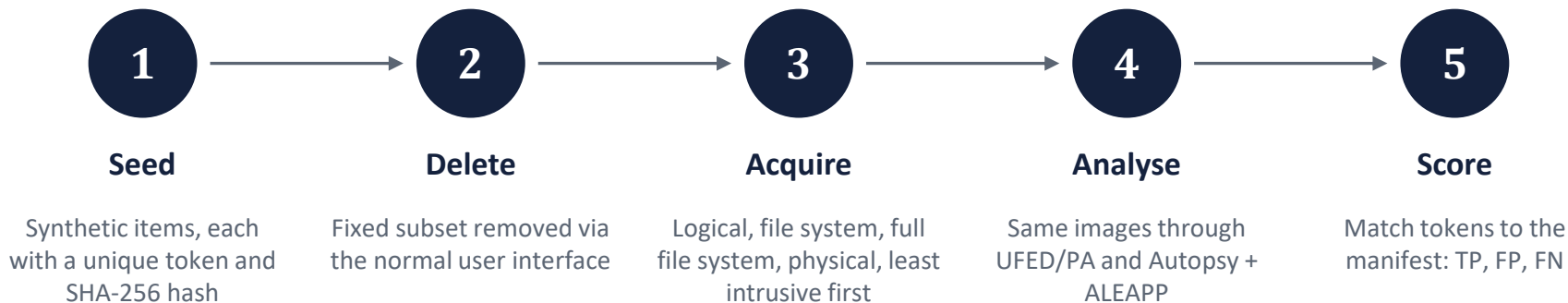
RQ4

How far do Android version, encryption and root explain variation?

RQ5

What do the error rates imply for evidential weight?

Planned Methodology



Metrics fixed before any data was collected

Recovery rate

Precision

Metadata fidelity

Integrity

Time & effort

What Was Actually Tested



Samsung Galaxy S25 Ultra (SM-S938B/DS)

- Android 16, Snapdragon SM8750, 512 GB
- Locked bootloader, not rooted
- After First Unlock, USB debugging on
- WhatsApp, Signal and Telegram (current versions)

390

seeded test messages
(130 per app)

42

deleted through the
app interface

2

tool chains on
identical material

Tool chains

- Commercial: Cellebrite UFED 4PC 7.76 + Physical Analyzer 7.73 (educational licence)
- Open source: ADB 1.0.41, ALEAPP v2026.4.1, Autopsy 4.23.1

Commercial Chain: Cellebrite UFED



6 extraction types offered

No Full File System option for this model; Physical required root

File System (Android Backup) failed twice

'ADB backup failed - shared memory partially extracted'

APK Downgrade not attempted

Replaces installed apps, so it alters the exhibit

Advanced Logical completed

46 min 42 s; IM, email and browsing reported as not supported

8,294

messages decoded by Physical Analyzer,
almost all SMS

0

WhatsApp, Signal or Telegram messages
recovered

Open-Source Chain: ADB, ALEAPP and Autopsy



Copy shared storage

adb pull of /sdcard, packed into two archives (29.3 GB) and hashed



Find WhatsApp backups

msgstore.db.crypt14 plus daily and incremental backups, all encrypted



ALEAPP crashed

Python RecursionError on the archive; fixed by extracting to a folder



Run Autopsy

225,247 files indexed; 0 messages, 0 deleted files

More material collected, but no more message content. Signal left nothing; Telegram left two empty folders.

Acquisition Outcome Matrix

Method	Chain	Outcome	Reaches app data?
Advanced Logical	UFED	Completed; IM not supported	No
File System (Backup)	UFED	Failed twice (ADB backup error)	No
File System (APK Downgrade)	UFED	Not attempted (alters exhibit)	-
Full File System	UFED	Not offered for this model	-
Physical	UFED	Requires root; not attempted	-
Shared-storage copy	ADB	Completed; 29.3 GB	No

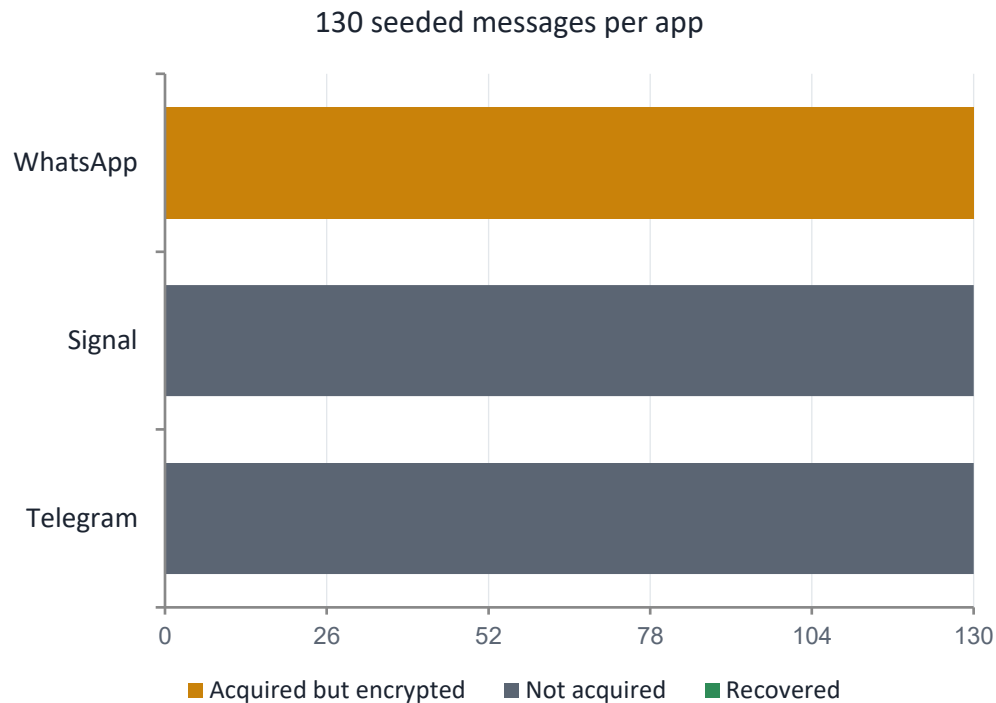
Only two methods produced output, and neither reaches /data/data, where deleted messages live.

Scoring Against the Ground Truth

0 / 42

deleted messages recovered by either chain

This does not prove the data was destroyed, or that either tool failed to parse it. The records were never presented to the tools.



Why Access Failed: Layered Barriers



Tool support No full file system method in the educational licence



Patch level July, then August 2026 patch; vendor methods lag behind



ADB backup deprecated Apps targeting API 31+ are excluded unless debuggable



Encryption + locked bootloader Unlocking to root wipes user data



App design WhatsApp backup key and Signal DB live in private storage



Samsung Auto Blocker Switched off; ruled out here, but a real casework risk



Removing any single barrier would not have changed the outcome. Device access, not tool capability, set the ceiling.

The Two Chains at the Logical Level

Cellebrite UFED

Acquisition	46 min 42 s
Analysis	Automatic decoding
Manual steps	0
Captured	SMS, calls, contacts, calendar
Transparency	Errors give no reason

VS

Autopsy + ALEAPP

Acquisition	About 1 h 35 min
Analysis	12 min ALEAPP + 3 h 5 min Autopsy
Manual steps	4
Captured	All shared storage, incl. WhatsApp backups
Transparency	Failures visible and traceable

Recommendations for Practitioners



Check access first

Record which methods the licence offers for the exact model and patch.



Freeze the device

Isolate from networks and defer updates; an update changes the exhibit.



Use both chains

Logical provider records plus a full copy of shared storage.



Qualify every zero

State the method, partitions reached and why deeper methods failed.



Protect file names

Use a file system that keeps Android names, or log renaming.



Keep the audit trail

Record who did each step when an acquisition is shared.

Limitations and Future Work



Limitations

- One device, one licence tier, two patch levels
- Corpus limited to three messaging apps
- No control device, so no precision figure
- Single retained run, not triplicate



Future work

- Re-run the design with full file system access (e.g. Inseyets or a pre-rooted research handset)
- Extend to SMS, media and app data, with a control device
- Measure deleted messages inside WhatsApp's encrypted backups
- Apply the same manifest design to iOS

CONCLUSION

On a current flagship, the answer was decided before either tool parsed anything: the deleted data was out of reach.

- Access, not tool choice, set the ceiling on a Galaxy S25 Ultra running Android 16
- Scoring against a manifest separates 'acquired but encrypted' from 'never acquired'
- A recovery rate means little without a statement of what the tools could reach

Thank you. Questions?