

Mobile Device Forensics and Encrypted Applications

*Evaluating Cellebrite UFED and UFED Physical Analyzer Against
WhatsApp, Signal, Telegram, and iMessage on Android and iOS*

Smit Brijeshkumar Patel

Enrollment: 2506590 | Level 7 | MSc Cyber Security and Digital Forensics

University of Wales Trinity Saint David – London Campus

Presented: Week 11 | April 2026

Research Context and Background

The Mobile Forensics Landscape

6.8B

Global smartphone users (2024) [1]

4B+

E2EE messaging app users globally [1]

E2EE

Default encryption on 4 major platforms [3]

36K+

Cellebrite UFED device profiles [7]

Why This Matters

With 6.8 billion smartphone users globally [1], mobile devices show up in nearly every serious criminal investigation. They are often the most important source of digital evidence.

E2EE as the Core Barrier

End-to-end encryption is default on WhatsApp, Signal, and iMessage, and partially available on Telegram [3]. The Signal Protocol Double Ratchet + X3DH provides per-message key rotation and forward secrecy, which makes retroactive decryption impractical [3].

Hardware Security Layers

Apple's Secure Enclave Processor (iOS) and Android's Trusted Execution Environment add hardware-level cryptographic barriers [4][5]. Cellebrite UFED is the most widely used extraction tool, but it is running into more and more E2EE limitations [2][7].

Current Developments and Literature Support

Key findings from 2019 to 2025

1

Encryption Evolution

WhatsApp uses AES-256 local DB encryption [8]; Signal uses SQLCipher with hardware-derived keys [3]; Telegram offers partial E2EE through Secret Chats only; iMessage relies on a Secure Enclave Processor-protected key chain [4]. Each app handles encryption differently, so they need to be analysed separately.

2

Mobile OS Security Advances

Android's hardware-backed keystore and full-disk encryption [5], combined with iOS Advanced Data Protection extending E2EE to iCloud backups [4], have made physical extraction much less reliable on current devices.

3

Forensic Tool Capabilities

Cellebrite UFED supports logical, file-system, physical and advanced extraction modes [7]. UFED Physical Analyzer decodes and parses application data into court-ready reports [2]. That said, how well these tools perform against current E2EE versions is not well documented [6].

4

Identified Literature Gap

No current peer-reviewed study provides a systematic, ground-truth-validated comparison of Cellebrite UFED performance across all four target applications on both Android 14/15 and iOS 17/18 simultaneously [6]. This research aims to fill that gap.

Research Problem Statement

Core Problem: We do not have solid, tested data on how much evidence Cellebrite UFED and UFED Physical Analyzer can actually recover from E2EE-protected communications on current Android and iOS platforms [6]. There is a gap between what these tools claim to extract and what is genuinely accessible.

1

Cryptographic Barrier

The Signal Protocol's per-message key rotation and SQLCipher-protected databases make decryption impractical without direct access to hardware keys [3]. WhatsApp's AES-256 local DB encryption [8] and iOS's Secure Enclave Processor [4] add more layers on top of that.

2

Rapid Obsolescence

Application and OS updates routinely modify database schemas, encryption implementations, and storage paths [6]. A forensic procedure validated against one version may fail entirely against the next release. Android and iOS both continuously tighten security architectures [4][5].

3

Legal Ambiguity

UK law still assumes investigators can compel providers to hand over data, but E2EE providers do not actually hold decryption keys. This raises real questions about whether current lawful access obligations are workable in practice [6].

Research Aim and Objectives

Objectives tied to the research problem

Research Aim: To test how well Cellebrite UFED and UFED Physical Analyzer can acquire and analyse digital evidence from WhatsApp, Signal, Telegram, and iMessage on Android 14/15 and iOS 17/18, and to produce practical recommendations for forensic practitioners based on the results.

O1

Systematic Literature Review

PRISMA review of mobile forensics, E2EE architectures and tool capabilities (2019–2025).
Specific: 4 platforms | Measurable: PRISMA protocol | Weeks 1–3

O2

Encryption Architecture Analysis

Analyse encryption and storage of WhatsApp [8], Signal [3], Telegram, iMessage [4] on Android [5] and iOS.
4 apps × 4 OS versions | Documented acquisition map

O3

Controlled Laboratory Experiment

Cellebrite UFED [7] and UFED Physical Analyzer [2] across 16 device-app combinations with ground-truth dataset.
Weeks 4–7 | Recovery rate, integrity, completeness, time

O4

Comparative Performance Evaluation

Standardised rubric: recovery rate, SHA-256 hash integrity, artefact completeness and acquisition time.
Quantitative metrics | Achievable with lab equipment

O5

Legal and Ethical Analysis

Review the legal and ethical rules around forensic access to encrypted mobile data in the UK [6].
UK jurisdiction | Weeks 8–9

O6

Best-Practice Framework

Bring together O1–O5 findings into a practical framework and policy recommendations.
Achievable | Practitioner-facing output



Literature Review - Key Findings and Gap

Four themes from the literature and where they leave us

T1 Mobile Forensics Evolution

The field has moved from basic SIM card extraction to confronting multi-layer encrypted architectures. Over 4 billion users now rely on encrypted platforms [1], and many older acquisition techniques simply no longer work [2][7].

T2 E2EE Application Architectures

Signal Protocol [3] combines X3DH with Double Ratchet for forward and future secrecy. WhatsApp uses AES-256 local DB [8]; Signal uses SQLCipher + hardware key [3]; iMessage uses SEP-protected key chain [4]. You cannot treat them as one problem.

T3 Cellebrite Tool Capabilities

Cellebrite UFED and UFED Physical Analyzer are the most widely used tools among practitioners [2][7]. Recovery rates against current E2EE versions are limited and largely untested in peer-reviewed literature [6]. No systematic cross-platform comparison exists yet.

T4 Legal and Ethical Context

There is real friction between individual privacy rights and law enforcement access needs [6]. E2EE now default on major platforms [3][8] creates practical and legal ambiguities around what forensic access is achievable and what is lawfully permissible under UK law.

The Gap: No existing empirical study compares Cellebrite UFED across all 4 apps on both Android 14/15 [5] and iOS 17/18 [4] at the same time [6].

Research Methodology - Design and Approach

Mixed-Methods | Experimental Design | Pragmatist Philosophy

1

Systematic Literature Review

PRISMA 2020 protocol
IEEE Xplore, ACM, Scopus
Focus: mobile forensics, E2EE [3][8],
Cellebrite [2][7], legal tensions [6]
Scope: 2019–2025

Weeks 1–3

2

Controlled Lab Experiment

16 virtual device image combinations
Android 14/15 [5] + iOS 17/18 [4]
virtual images WhatsApp [8] / Signal
[3] / Telegram / iMessage [4] Sourced
from publicly available online
repositories Cellebrite UFED [7] + UFED
PA [2]

Weeks 4–7

3

Document Analysis

Legal and ethical frameworks
Thematic coding (NVivo)
Privacy–safety balance [6]
UK jurisdiction focus

Weeks 8–9

4

Synthesis & Recommendations

Triangulate all phases
Best-practice framework
Draft thesis chapters
Practitioner guidance

Weeks 9–10

Research Materials, Tools and Data Collection

Cellebrite UFED [7]

Hardware extraction unit used by most forensic labs. Supports logical, file-system, physical and advanced acquisition across 36,000+ device profiles. This is the primary acquisition tool for all 16 device-application combinations in the study.

UFED Physical Analyzer [2]

Works alongside the UFED hardware. Decodes acquired datasets, parses application artefacts, reconstructs timelines and produces evidential reports. Used for all application artefact decoding in this study.

Supporting Tools

SQLite Browser | Python 3 (pandas, hashlib) | NVivo | Faraday cage

1

Source and Configure Virtual Device Images

Source and Configure Virtual Device Images Android 14 & 15 [5] + iOS 17 & 18 [4] virtual images sourced from publicly available online repositories. Install WhatsApp [8], Signal [3], Telegram, iMessage.

2

Generate Ground-Truth Dataset

200+ messages, 20 images, 10 audio/video, 10 call records per app per device. Researcher-generated only - no real personal data.

3

Acquire via Cellebrite UFED [7]

All acquisition modes. Faraday-shielded environment. SHA-256 hash recorded at acquisition.

4

Decode with UFED Physical Analyzer [2]

Parse all acquired images. Export artefacts. Compare against ground-truth dataset.

5

Evaluate Against Rubric

Recovery rate, data integrity, artefact completeness, acquisition time. Statistical analysis in Python.

Evaluation Framework and Metrics

How performance will be measured across all 16 device-application combinations

M1

Recovery Rate (%)

Ground-truth artefacts (messages, media, metadata) successfully recovered as a % of total known artefacts. Measured per application per platform, with focus on differences between E2EE implementations [3][8] and Android [5] vs iOS [4].

Count recovered ÷ total ground-truth × 100

M2

Data Integrity

SHA-256 hash verification of all recovered files against originals, confirming no corruption or data loss during acquisition or decoding [2][7]. Without this, evidence is unlikely to be admissible in UK courts.

Hash mismatch rate per acquisition - 0% = full integrity

M3

Artefact Completeness

Proportion of message metadata fields correctly decoded by UFED Physical Analyzer [2]: timestamps, sender/recipient IDs, delivery status, read receipts, media captions. How much you get back depends heavily on each app's encryption [3][8][4].

Per-field completeness score (%) compared across all app outputs

M4

Acquisition Time

Elapsed time from acquisition initiation through to completion and decoding [7]. This matters because investigators often have limited time with a device before they have to return it.

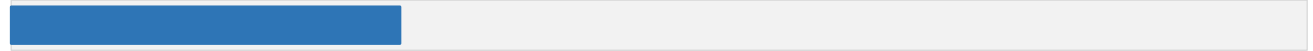
Stopwatch-measured - mean and range per device-app combination

Project Planning and Resource Management

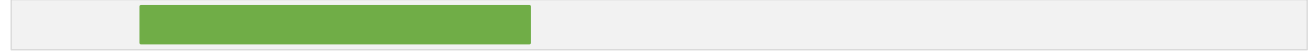
10-Week Timeline (2.5 Months) | Gantt Chart

W1 W2 W3 W4 W5 W6 W7 W8 W9 W10

Ph.1: Literature Review



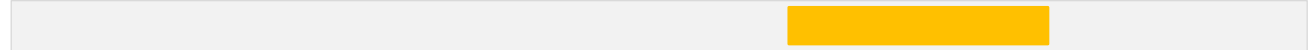
Ph.2: Lab Setup & Ethics



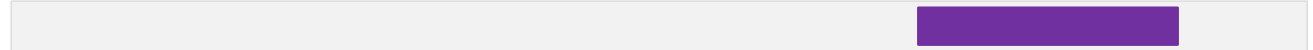
Ph.3: Data Collection (UFED)



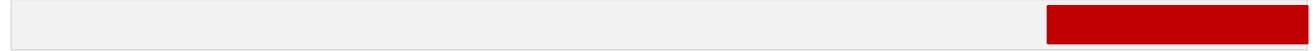
Ph.4: Data Analysis



Ph.5: Legal & Ethical Analysis



Ph.6: Write-up & Submission



Test Devices

Virtual Device Images Android 14/15 [5]
+ iOS 17/18 [4] (sourced freely from
online repositories)

Cellebrite UFED [7]

UFED Touch2 or Premium
(UWTSD Forensics Lab licence)

UFED Physical Analyzer [2]

Current licensed version
(UWTSD institutional access)

Lab Infrastructure

Faraday cage, isolated network
Encrypted 1TB storage

Expected Outcomes, Impact and Limitations

Realistic Tool Benchmark

1

Hands-on comparison of Cellebrite UFED [7] and UFED PA [2] across all 4 E2EE apps on Android 14/15 [5] and iOS 17/18 [4] at the same time.

Encryption Analysis Map

2

Documented forensic acquisition points and barriers for WhatsApp [8], Signal [3], Telegram and iMessage [4] that practitioners can actually use.

Legal Framework Analysis

3

Critique of how well existing legal frameworks handle encrypted app forensics, with reform recommendations backed by test results [6].

Best-Practice Framework

4

Tested, practical guidance for forensic investigators working with encrypted mobile applications [2][7].

Practitioners

Up-to-date tool guidance for UK law enforcement [2][7]

Academic

Addresses an untested area in the literature; reproducible methodology [6]

Policy

Evidence base for proportionate lawful access legislation [3][8]

Societal

Adds tested evidence to the privacy vs. public safety debate [6]

Key Limitations

Results reflect specific tool/app versions at one point in time frequent updates limit long-term generalisability [3][8][7]. Virtual device images may not fully replicate hardware-level security features such as the Secure Enclave Processor and TEE. UFED Premium advanced extraction subject to licensing constraints. Legal analysis limited to UK jurisdiction.

References (IEEE Format)

- [1] Statista, 'Smartphone users worldwide 2014–2029,' Statista, 2024.
- [2] Cellebrite Ltd., 'UFED Physical Analyzer: Technical Overview,' Tech. Rep., 2024.
- [3] M. Marlinspike & T. Perrin, 'The Double Ratchet Algorithm,' Signal Foundation, 2016.
- [4] Apple Inc., 'iOS Security Guide,' Apple Inc., Tech. Rep., 2024.
- [5] Google LLC, 'Android Security Bulletins,' Google LLC, 2024.
- [6] N. Mee & J. Nurse, 'Challenges of mobile device forensics with encrypted apps,' Comput. Secur., vol. 111, 2021.
- [7] Cellebrite Ltd., 'Cellebrite UFED: The Industry Standard for Mobile Forensics,' Product Brief, 2024.
- [8] WhatsApp Inc., 'WhatsApp Encryption Overview,' Tech. White Paper, 2023.

Conclusion

This research is the first hands-on comparison of Cellebrite UFED and UFED Physical Analyzer across WhatsApp, Signal, Telegram, and iMessage on Android 14/15 and iOS 17/18. No peer-reviewed study has tested this combination before.

The results should give UK law enforcement up-to-date guidance on what these tools can actually do, offer a methodology other researchers can replicate, and provide evidence that can inform lawful access policy.

Thank You