

A Practitioner's Perspective on the Complementary Use of Cellebrite UFED and Oxygen Forensic Detective in Mobile Device Forensics

Iyeru Godsglory Oluwole

Independent Corrupt Practices and Other Related Offences
Commission, Nigeria
Digital Forensics Expert

*Corresponding Author: **Iyeru Godsglory Oluwole**

Abstract

Mobile devices now hold an extraordinary record of a person's life — who they contacted, where they went, what they searched for, and often the sequence in which key events occurred. As the volume and complexity of mobile evidence grows, examiners rely increasingly on specialized forensic platforms to acquire process, interpret, and present that evidence.

This paper offers a practitioner's perspective on the complementary use of Cellebrite UFED and Oxygen Forensic Detective (OFD) in mobile device examinations. It does not attempt to declare one platform superior. Instead, drawing on roughly a decade of hands-on experience with both, it argues that each platform's strengths and limitations can be deliberately exploited to produce a more complete, efficient, and defensible examination. Particular attention is given to differences in extraction workflow, processing efficiency, artifact presentation, geospatial and link analysis, timeline reconstruction, and cross-platform verification. In the author's operational experience, Oxygen has, in comparable circumstances, processed certain datasets substantially faster than Cellebrite-based workflows — in some cases by a factor approaching eight. This is offered as a practitioner observation tied to specific casework conditions rather than a universal performance claim, since processing speed depends heavily on device architecture, extraction method, data volume, hardware, software version, and artifact complexity. The central proposition is that the relative weakness of one platform can be finding, while disagreement flags something — an artifact,

Article DNA

Article Type:

Original research article

DOI:

10.5281/zenodo.23065954

Article History:

Received: 16-09-2026

Accepted: 20-09-2026

Published: 30-09-2026

Keywords:

Mobile device forensics;
Cellebrite UFED; Oxygen
Forensic Detective; digital
evidence; forensic validation;
cross-validation; digital
intelligence; geospatial
analysis; link analysis;
forensic examination.

How to Cite

Iyeru Godsglory Oluwole.
(2026). A Practitioner's
Perspective on the
Complementary Use of
Cellebrite UFED and Oxygen
Forensic Detective in Mobile
Device Forensics. *UAR Journal
of Multidisciplinary Studies
(UARJMS)*, 2(9), 1–11.
<https://doi.org/10.5281/zenodo.23065954>

License Information

Copyright © 2025 The
Author(s). This is an open-
access article distributed under
the terms of the [Creative
Commons Attribution License
\(CC BY 4.0\)](#), which permits
unrestricted use, distribution,
and reproduction in any
medium, provided the original
author and source are credited.

***Related declarations are
provided in the final section of
this article.*

The practical strength of the other, and that using both to independently process the same extraction provides a form of forensic cross-validation: agreement between platforms strengthens confidence in a parser, an extraction characteristic — that warrants closer scrutiny. The paper proposes a Bidirectional Forensic Cross-Validation (BFCV) Model, in which evidence can move in either direction between the two platforms rather than following a fixed, vendor-dependent path. It argues that the future of mobile forensics should not be framed around finding a single “best” platform, but around building scientifically defensible workflows in which complementary technologies maximize evidence recovery, minimize analytical blind spots, and strengthen confidence in forensic conclusions.

Introduction

There was a time when examining a mobile phone meant looking for call records, text messages, contacts, and photographs. That time has passed. The modern smartphone is effectively a digital extension of its user: it records communications, movements, relationships, searches, media, financial activity, application interactions, and increasingly, fragments of activity the user never deliberately created. A single device can answer questions of who, what, when, where, and how.

But availability of data does not translate automatically into understanding. A device may hold thousands or millions of artifacts; the challenge is not recovering them but determining which matter, how they relate to one another, whether they are reliable, how they fit the investigative chronology, and whether conclusions drawn from them can withstand scrutiny. This is where forensic software becomes decisive.

Over roughly a decade of practical casework, I have worked extensively with two platforms central to this discussion: Cellebrite UFED and Oxygen Forensic Detective. I have extracted with both, processed evidence with both, and — importantly — used one to verify the work of the other. That experience has led me away from the conventional question of which platform is “better,” and toward a different conclusion: I do not regard Cellebrite UFED and Oxygen Forensic Detective as mutually exclusive tools. I regard them as complementary.

This paper is not a product review, nor an attempt to promote one commercial solution over another. It is an account of what happens when an examiner recognizes that two platforms may approach the same digital evidence differently, and deliberately uses those differences to strengthen the examination. In forensic science, differences between instruments are not necessarily weaknesses — sometimes they are precisely what makes independent verification possible.

2. Acquisition and Analysis: Two Related but Distinct Problems

The modern digital forensic laboratory faces two related but separate problems: gaining access to evidence, and understanding the evidence once obtained. An examiner can spend considerable effort overcoming device restrictions and recovering a large extraction, only to find that making sense of the resulting dataset is the harder task. Conversely, an analytical environment may offer excellent visualization and correlation tools that are of little use if the examiner cannot first obtain the underlying data.

Cellebrite UFED has long been associated with sophisticated acquisition capability, offering multiple extraction approaches — including physical and full-file-system acquisition — depending on the device and circumstances. Oxygen Forensic Detective, while it also performs acquisition, places greater emphasis on bringing extracted data into an integrated analytical environment, with timeline analysis, geolocation and mapping, link analysis, and cross-source examination. The practical implication is that the examination does not end when the extraction does — in many investigations, that is where the real work begins.

3. From Extraction to Intelligence

One of the clearest changes I have observed over the years is the widening gap between data extraction and investigative intelligence. An extraction can produce enormous volumes of information — tens of thousands of messages and call records, thousands of photographs, application databases, location artifacts, browser records, cloud data — but volume is not the same as intelligence. The examiner still has to determine who communicated with whom, when, and where; whether the same individuals appear across different applications; whether multiple devices converge on the same locations; and what sequence of events the combined evidence supports.

This is where Oxygen's analytical environment has proven particularly valuable in my experience: its timeline, geospatial, link-analysis, and visualization tools help transform large quantities of extracted artifacts into recognizable patterns. Put simply, extraction tells us what data can be recovered; analysis helps us understand what that data means. The two functions are related, but not identical.

4. Practical Experience: Using Both Platforms Together

Technical papers often discuss forensic platforms purely through specifications, which has value but can miss what actually happens at the examiner's workstation. In practice, the questions that

matter are practical ones: How quickly can I get the information I need? How much manual intervention is required? Can I see the relationship between artifacts, follow a suspect's movement, or identify a connection that was not obvious in the raw extraction? Can I reproduce an important finding on another platform — and if two platforms disagree, why?

My experience with both platforms has produced a strong preference for using them together rather than forcing an artificial choice. In some cases, Cellebrite has provided the acquisition capability an examination required, after which the evidence became far more useful once processed in Oxygen. In others, Oxygen handled acquisition or processing, and Cellebrite subsequently offered an independent means of examining or corroborating the findings. This two-way approach has been particularly useful for significant findings that may ultimately support an investigative or evidential conclusion, and it forms the practical foundation of this paper.

5. Complementary Strengths, Not Opposing Camps

Cellebrite UFED is not the enemy of Oxygen, and Oxygen is not a replacement for Cellebrite. An examiner using both does not need to abandon one for the other; the more useful question is what each platform can contribute to a particular examination. Cellebrite's acquisition architecture is valuable when the central challenge is obtaining data from a device; Oxygen's analytical environment is valuable once that data needs to be organized and interpreted. Oxygen's ability to bring different forms of information into analytical relationships can also expose patterns not readily visible through an acquisition-oriented workflow alone.

The relationship, then, is not Cellebrite versus Oxygen but Cellebrite plus Oxygen — and, in appropriate circumstances, a cycle of Cellebrite → Oxygen → Cellebrite or Oxygen → Cellebrite → Oxygen. That workflow deserves more attention than the conventional software comparison.

6. Independent Verification and the Forensic Complementarity Principle

One of the strongest lessons from practical casework is that independent verification matters. When a finding may be significant, I do not consider it sufficient that one platform alone produced it; where resources and procedure permit, the finding should be subjected to additional scrutiny using the second platform. If Cellebrite identifies an artifact, Oxygen can provide an

independent environment in which to examine it, and vice versa. Agreement between platforms strengthens confidence; disagreement is itself informative, prompting questions about whether the extraction, parser, application version, artifact interpretation, timestamp handling, or software version differs between the two results. This is a far healthier forensic posture than assuming the first result produced is automatically correct — a position broadly consistent with SWGDE guidance recognizing the value of using multiple forensic tools, including using a second tool to provide additional data or corroborate results (Scientific Working Group on Digital Evidence [SWGDE], 2024).

This experience supports what might be termed the Forensic Complementarity Principle: the forensic value of a digital examination may be increased when complementary platforms are deliberately deployed to exploit differences in acquisition, processing, interpretation, visualization, and validation capability. The principle does not imply either platform is inherently weak — only that no single platform should be expected to be optimal for every task, device, application, and investigative question, any more than a laboratory would rely on a single scientific instrument for every purpose. Independent methods provide corroboration, alternative interpretation, additional recovery, error detection, quality assurance, and greater overall confidence, a logic consistent with the broader digital forensics literature on differential and multi-source analysis (Garfinkel et al., 2012).

7. The Bidirectional Forensic Cross-Validation (BFCV) Model

This leads to the central model proposed in this paper. Unlike a conventional arrangement in which one platform is treated as primary and the other as backup, BFCV treats both platforms as potentially independent examination environments, with evidence able to move in either direction depending on forensic circumstances:

Model A: Device → Cellebrite UFED → Extraction → Oxygen Forensic Detective → Independent processing and analysis → Cross-validation.

Model B: Device → Oxygen Forensic Detective → Extraction → Cellebrite UFED → Independent processing and analysis → Cross-validation.

The principle is bidirectional rather than hierarchical, which avoids simply substituting one form of tool dependency for another.

8. Practical Illustrations

8.1 Acquisition pathways. Cellebrite has traditionally offered a strongly acquisition-oriented environment, with distinct acquisition methods — including physical and full-file-system extraction where supported — depending on device, operating system, and security posture. Oxygen, by contrast, presents a more integrated environment in which acquisition results move relatively naturally into processing and analysis. Neither approach is inherently superior; they simply encourage the examiner to think about the evidence differently. An examiner asking “exactly what type of extraction have I obtained?” benefits from Cellebrite's explicit categorization; one asking “what can I learn from everything I have obtained?” benefits from Oxygen's integrated environment. The two platforms are solving related but not identical problems.

8.2 Android and iOS considerations. Android and iOS devices differ substantially in security architecture, file structure, application behavior, and acquisition possibilities, and even within one operating system, device model, chipset, OS version, and security configuration affect what is recoverable. It is not good practice to assume a single acquisition method will always suffice; the examiner must understand the device, the available acquisition options, and the evidential objective before choosing a pathway. Cellebrite's depth of device-acquisition support is valuable here, while Oxygen becomes particularly valuable once the resulting data needs to be rapidly processed and interpreted. Acquisition capability and analytical capability should not be confused with one another — a successful extraction is only the beginning of the examination.

8.3 Geospatial analysis. Geospatial evidence illustrates the difference between recovering evidence and understanding it especially well. A coordinate on its own is an artifact; the investigative value comes from context — for example, discovering that several devices repeatedly occupied the same area during the period preceding a transaction under investigation. Oxygen's mapping and Dynamic Mapping capabilities allow location artifacts to be examined spatially rather than as isolated records, letting the examiner see the investigation rather than simply read it. A map can reveal frequently visited locations, movement patterns, proximity between individuals, possible meeting points, and deviations from established patterns — but a map is an analytical aid, not proof; underlying artifacts must still be validated and interpreted within the facts of the case.

8.4 Link analysis. Where a traditional examination might produce a simple contact list (A→B, B→C, C→D) that the investigator must interpret manually, a link-analysis environment makes relationships directly visible. Oxygen's graph-based analytical tools are particularly useful here, especially in cases involving organized criminal activity, corruption, cybercrime, or coordinated fraud, where the relevant question shifts from “did these people communicate?” to “what network emerges when all relevant communications and relationships are considered together?” Individually unremarkable devices can, considered collectively, reveal a network — moving the examination from device-centric to relationship-centric, and ultimately network-centric, analysis. This is one of the clearest examples of Oxygen's analytical strengths complementing Cellebrite's acquisition strengths.

8.5 Visualization and its limits. Graphics in forensic work are sometimes dismissed as cosmetic; in practice, with very large datasets, visualization substantially affects an examiner's ability to recognize patterns — a timeline can reveal a sequence difficult to see in raw timestamps, a map can reveal geography difficult to see in a spreadsheet, and a link graph can expose a network that would otherwise take hours to reconstruct manually. Its value lies in reducing cognitive load and surfacing relationships within complex evidence, which matters more as devices generate more data than an examiner can reasonably review by hand.

That value comes with a caution: visual clarity is not evidential certainty. Every significant visual conclusion must be traceable back to its underlying artifact — the communication, application or database, timestamp, source device, and extraction method behind a link on a graph, or the source, accuracy, and timestamp behind a point on a map, along with whether it reflects an actual device location or a merely stored one, and whether other evidence corroborates the interpretation. Powerful visualization must be paired with disciplined forensic methodology.

9. When the Tools Disagree

The greatest value of using both platforms is not necessarily when they agree — it is when they challenge each other. If Cellebrite and Oxygen independently identify the same artifact, that is valuable; but when they disagree, the correct response is neither “Oxygen is wrong” nor “Cellebrite is wrong.” It is to ask why the results differ. That question can lead to examining acquisition methodology, extraction completeness, database availability, parser interpretation, application or OS version, timestamp conversion, treatment of deleted data, encryption, software

version, or artifact derivation. Disagreement, in other words, becomes a forensic lead rather than a problem to be dismissed.

10. Limitations of This Paper

This paper is a practitioner reflection grounded in approximately a decade of casework rather than a controlled experimental study, and its conclusions should be read with that distinction in mind. Several limitations are worth stating explicitly.

First, the observations reported here — including the approximate eightfold processing-speed differential noted in the abstract — derive from a single examiner's operational experience rather than a systematic, blinded, or statistically powered comparison. Processing speed, artifact recovery completeness, and parsing accuracy are all sensitive to device model, chipset, operating system version, extraction type, dataset size, hardware configuration, and the specific software build in use at the time; figures observed in one casework context will not necessarily reproduce in another, and both platforms are under continuous vendor development, so relative performance can shift between software versions.

Second, a single-examiner retrospective account carries an inherent risk of confirmation bias: cases in which cross-validation confirmed or refined a finding may be more memorable, or more readily recalled, than cases in which it added little. No attempt has been made here to quantify how often cross-validation changed an outcome versus merely confirming it.

Third, this paper does not include a structured dataset, a reproducible test methodology, or independent peer replication of the specific comparisons described. It is offered as a practitioner hypothesis and framework — the Bidirectional Forensic Cross-Validation (BFCV) Model and the Forensic Complementarity Principle — intended to be tested, refined, or challenged by controlled research rather than treated as an already-validated finding.

Fourth, the discussion is limited to two specific commercial platforms. While the underlying logic is likely to generalize to other forensic tool pairs, that generalization is itself untested here and should not be assumed.

11. Implications for Practice and Recommendations for Future Research

Notwithstanding the limitations above, the practical experience described in this paper carries several implications for laboratory practice and points toward specific directions for future research.

11.1 For laboratory practice. Laboratories handling high-stakes findings — those likely to be contested, to carry significant evidential weight, or to support a charging or prosecutorial decision — may benefit from formalizing independent secondary-tool verification as a standard operating procedure rather than an ad hoc practice left to individual examiner discretion. This is consistent with, and operationalizes, existing SWGDE guidance on the value of using multiple tools for validation and corroboration (SWGDE, 2024) and with NIST guidance on mobile device forensic procedure (Ayers et al., 2014). Standard operating procedures could specify which categories of findings require cross-tool verification, how disagreements are documented, and how an examiner should escalate an unresolved discrepancy.

11.2 For tool selection and procurement. Laboratories evaluating forensic platform procurement or renewal may benefit from assessing tools as complementary components of a workflow rather than as competing, mutually exclusive purchases, particularly where budget allows maintaining more than one platform for cross-validation on significant matters.

11.3 For future research. The observations in this paper point toward several concrete research directions. A structured, multi-examiner, multi-laboratory benchmarking study — following NIST Computer Forensics Tool Testing (CFTT) methodology (National Institute of Standards and Technology, n.d.) — could quantify processing time, artifact recovery completeness, and parsing accuracy across a defined set of devices and datasets, replacing anecdotal performance observations with reproducible figures. A second avenue would formally test the BFCV model itself: does bidirectional cross-validation measurably change examiner conclusions, error rates, or confidence calibration compared to single-platform workflows, in a design similar in spirit to differential forensic analysis approaches described in the digital forensics literature (Garfinkel et al., 2012; Hargreaves et al., 2024)? A third avenue would extend the complementarity framework beyond Cellebrite and Oxygen to other tool pairs used in mobile and computer forensics, to test whether the principle generalizes or is specific to the acquisition-versus-analysis division observed between these two platforms.

11.4 For standardization. Finally, the development of a standardized template for documenting cross-tool agreement and disagreement — what was compared, on which platform versions, with

what result, and how any discrepancy was resolved — would improve the reproducibility and evidential defensibility of cross-validation work across the field, rather than leaving it to individual laboratory or examiner convention.

12. Conclusion: Two Tools, One Truth

The objective of using two forensic platforms is not to make them produce identical screens. It is to determine whether the underlying evidence can withstand examination from more than one forensic perspective. When both platforms independently recover and interpret a significant artifact consistently, confidence in that finding increases. When one platform adds context the other lacks, that context can improve investigative interpretation. When the platforms disagree, the discrepancy itself is a reason for further examination.

Two tools do not necessarily produce two versions of the truth. Properly used, they provide two opportunities to interrogate the same evidence. That is the essence of forensic cross-validation, and it is the reasoning behind the Bidirectional Forensic Cross-Validation Model proposed here: rather than a fixed “primary tool, backup tool” hierarchy, the examiner moves between Cellebrite and Oxygen as a finding requires confirmation, deeper analysis, or explanation — Cellebrite ↔ Oxygen, rather than a one-way path in either direction. The future of mobile device forensics should be framed not around identifying a single best platform, but around building scientifically defensible workflows in which complementary technologies maximize evidence recovery, minimize analytical blind spots, and strengthen confidence in forensic conclusions.

Disclosure Statement

The author has no financial or commercial relationship with Cellebrite, Oxygen Forensics, or any competing vendor. The views expressed in this paper are the author's own, based on personal professional experience, and do not represent the official position of any employer, agency, or organization with which the author is or has been affiliated.

Article Publication Details

This article is published in the **UAR Journal of Multidisciplinary Studies (UARJMS)**, ISSN 3049-4346 (Online). In Volume 2 (2026), Issue 9 (September)

The journal is published and managed by **UAR Publisher**.

References

1. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101, Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-101r1>
2. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
3. Garfinkel, S., Nelson, A., & Young, J. (2012). A general strategy for differential forensic analysis. *Digital Investigation*, 9, S50–S59. Presented at the Digital Forensics Research Workshop (DFRWS) 2012 USA.
4. Hargreaves, C., Nelson, A., & Casey, E. (2024). An abstract model for digital forensic analysis. *Forensic Science International: Digital Investigation*. Presented at DFRWS EU 2024.
5. National Institute of Standards and Technology. (n.d.). Computer Forensics Tool Testing Program (CFTT): Mobile forensics. Retrieved September 2026, from <https://csrc.nist.gov/projects/mobile-forensics>
6. Scientific Working Group on Digital Evidence. (2024). Minimum requirements for testing tools used in digital and multimedia forensics (Version 18-Q-001-2.1). <https://www.swgde.org>