A Confidence-Aware Multi-Layer Framework for Drone Forensic Inference Using Heterogeneous Digital Evidence Sources and Flight Logs Analysis

Nidhiba Parmar, Naveen Kumar Chaudhary
School of Cyber Security and Digital Forensics, National Forensic Sciences University, Gandhinagar, India

***Abstract*—The increasing use of unmanned aerial vehicles (UAVs) in criminal and adversarial contexts has created new challenges for digital forensic investigations. Current UAV forensic research primarily emphasizes artefact extraction and platform-dependent analysis, while insufficient attention has been given to uncertainty modelling and confidence quantification in forensic inference. This study addresses this methodological gap by proposing a confidence-aware multi-layer UAV forensic framework designed to support legally defensible forensic conclusions. The framework integrates chip-off memory acquisition, logical flight log analysis, companion mobile device artefact examination, and wireless trace correlation within a unified analytical architecture. Physics-based flight trajectory reconstruction and cross-device temporal alignment algorithms enhance reproducibility and platform independence. To reflect varying levels of evidentiary reliability, a structured evidence-weighting approach is introduced alongside a novel Forensic Confidence Index (FCI) that quantifies evidentiary support without implying absolute certainty. Validation using a Yuneec Typhoon Q500 4K dataset demonstrates feasible trajectory reconstruction, temporal correlation, and confidence-constrained attribution under realistic investigative conditions. By explicitly incorporating uncertainty modeling and confidence articulation into UAV forensic workflows, the proposed framework improves scientific rigor, transparency, and legal defensibility while providing a scalable foundation for future cyber-physical forensic investigations.**

Keywords*—*UAV forensics; drone investigations; forensic inference; confidence quantification; flight log analysis; digital forensic framework

I. Introduction

The operational footprint of unmanned aerial vehicles (UAVs) has expanded beyond recreational and commercial domains into increasingly adversarial and criminal contexts, including illicit surveillance, cross-border smuggling, critical-infrastructure reconnaissance, and targeted cyber-physical intrusions [1]. The proliferation of UAV use has concomitantly increased the importance of drones from artefacts to a primary vector of evidentiary importance in digital forensics investigations [2]. However, contemporary UAV forensic methodology is largely data-centric (focusing more on extracting information from data than on forensic inference), which limits its probative and explanatory value in high-stakes investigative and judicial settings [3], [4], [5].

Recent UAV forensic studies between 2023 and 2025 have shown significant progress in terms of systematic cataloguing of the artefact locations, demystifying proprietary flight logs, and retrieving multimedia and telemetry information from widely used drone platforms, especially the DJI and, to a lesser extent, Yuneec and Parrot ecosystems [6], [7], [8]. However, these contributions are less than comprehensive in this regard; they outline the data that can be obtained from such types of evidence, but not the degree of confidence with which such data can be used to support forensic attribution, a point in time, or the association with an operator. Consequently, many essential forensic issues related to evidentiary reliability, cross-source consistency, and the propagation of uncertainty are often left implicit or unanswered. A critical, unanswered problem in modern UAV forensics is the absence of formal mechanisms for quantifying evidentiary confidence when analyzing diverse, heterogeneous sources, including chip-off memory, removable storage, companion mobile devices, and wireless communication traces.

Specifically, this study makes the following contributions:

- Proposes a unified multi-layer UAV forensic architecture integrating physical, logical, companion-device, and wireless evidence sources.
- Introduces formal algorithms for flight path reconstruction and cross-device temporal alignment.
- Develops uncertainty-aware evidence weighting model grounded in forensic reliability principles.
- Defines a novel Forensic Confidence Index (FCI) to quantify attribution strength.
- Validates the framework through a Yuneec Typhoon Q500 4K case study while ensuring device-agnostic generalizability.

Although UAV forensic research has advanced in artefact extraction and platform-specific analysis, there remains a lack of structured frameworks for confidence-based forensic inference across heterogeneous evidence sources. Existing approaches rarely incorporate uncertainty modelling or reliability weighting, which limits the scientific rigor and legal defensibility of forensic conclusions. This study addresses this gap by proposing a confidence-aware multi-layer UAV forensic framework integrating diverse evidence sources with explicit confidence quantification.

The remainder of this study is organized as follows: Section II reviews related work and identifies key

methodological gaps in UAV forensic research. Section III presents the theoretical foundation underlying confidence-aware forensic inference. Section IV describes the proposed multi-layer UAV forensic framework and methodological approach. Section V details the associated analytical models and algorithms. Section VI presents the case study validation using the Yuneec Typhoon Q500 4K dataset. Section VII discusses comparative and theoretical implications of the findings. Section VIII addresses generalization, admissibility, and practical deployment considerations. Section IX outlines study limitations and future research directions, and finally, Section X concludes the study.

II. Related Work and Gap Synthesis

The rapid proliferation of unmanned aerial vehicles (UAVs) across civilian, commercial, and adversarial domains has significantly increased the importance of UAV digital forensic investigations. Recent research has focused on artefact extraction, flight log interpretation, and forensic framework development; however, methodological maturity in forensic inference, particularly regarding uncertainty quantification and confidence modeling, remains limited.

Recent UAV forensic studies emphasize systematic artefact acquisition and device-specific forensic analysis. For example, recent forensic investigations of modern DJI drones have demonstrated the feasibility of extracting telemetry logs, encryption structures, and internal storage artefacts through structured parsing frameworks [9]. Similarly, controller-level forensic analysis has shown that remote controller data can reveal pilot identity, pairing timestamps, and operational locations, thereby expanding evidentiary scope beyond onboard storage [10].

Several contemporary studies have proposed broader forensic frameworks. A conceptual digital forensic investigation model for UAVs was introduced to guide the identification, preservation, analysis, and documentation of drone evidence [11]. Likewise, recent survey research has categorized UAV forensic artefacts, tools, and frameworks while identifying unresolved research themes such as evidence standardization and reproducibility [12]. These studies highlight the growing recognition of UAV forensics as a specialized domain but also indicate persistent methodological fragmentation.

Emerging research between 2024 and 2025 has increasingly focused on integrating diverse forensic data sources. Case studies involving DJI Mini and Phantom drones demonstrate that correlating internal storage, controller data, and flight telemetry can improve event reconstruction accuracy [13], [14]. Additionally, recent investigations into live and static digital evidence traceability have emphasized challenges related to data integrity, repeatability, and evidentiary admissibility [15]. These challenges are particularly critical when forensic findings are presented in legal contexts.

Innovative methodological approaches are also emerging. Digital twin technology has recently been explored for drone accident reconstruction, enabling simulation-based validation of forensic hypotheses and improved investigative accuracy [16]. Metamodeling approaches have likewise been proposed to standardize UAV forensic investigation processes across heterogeneous platforms [17]. Furthermore, recent cybersecurity-oriented forensic frameworks advocate real-time anomaly detection and automated evidence preservation mechanisms for UAV ecosystems [18].

Recent literature also highlights operational and legal challenges. Law-enforcement-focused research indicates that drone forensic investigations face difficulties related to proprietary software, encryption, anti-forensic techniques, and privacy concerns [19]. Similarly, studies on tool-based forensic analysis emphasize the need for standardized methodologies to improve evidentiary reliability and legal defensibility [20].

Another significant development is the exploration of multi-source data correlation. Studies involving industrial and security applications demonstrate that combining flight logs, SD card data, and mobile application artefacts can support attribution and event reconstruction [21]. Transformer-based approaches have also been proposed to link mobile devices with UAV activity, indicating increasing interest in AI-assisted forensic correlation [22].

Despite these advancements, several limitations persist. First, most existing studies focus on artefact extraction rather than forensic inference. Second, uncertainty modeling and confidence quantification are rarely explicitly addressed. Third, cross-layer evidence fusion is typically informal and lacks structured reliability weighting. Finally, empirical validation often relies on single case studies or platform-specific datasets, limiting generalizability.

Therefore, a critical methodological gap exists in UAV forensic research: the absence of a confidence-aware, multi-layer forensic inference framework capable of integrating heterogeneous evidence sources while explicitly modeling uncertainty. Addressing this gap is essential for improving the scientific rigor, transparency, and legal defensibility of UAV forensic investigations.

The present study addresses these limitations by proposing a structured multi-layer UAV forensic framework incorporating physics-based trajectory reconstruction, cross-device temporal alignment, explicit evidence reliability weighting, and a novel Forensic Confidence Index (FCI). This approach moves beyond artefact extraction toward confidence-aware forensic inference suitable for investigative and judicial applications.

A. Methodological and Theoretical Weaknesses

Despite substantial progress in UAV forensic artefact extraction and analytical tool development, several methodological limitations remain. First, uncertainty associated with UAV forensic data is rarely formally modelled, even though sensor noise, timestamp drift, synchronization errors, and partial data loss are inherent characteristics of cyber-physical evidence. Second, structured evidence fusion frameworks capable of systematically integrating heterogeneous sources with differing reliability profiles remain limited. Third, there is no widely accepted mechanism for expressing the strength of forensic attribution as a measurable confidence level, despite increasing emphasis on confidence reporting in forensic admissibility discussions.

These limitations constrain the evolution of UAV forensics from a primarily technical data extraction activity toward a mature forensic science discipline grounded in transparent inference and defensible interpretation. To further illustrate these methodological gaps, Table I presents a comparative analysis of recent UAV forensic studies, highlighting the limited treatment of uncertainty modelling, confidence quantification, and multi-layer evidence integration.

TABLE I. COMPARATIVE ANALYSIS OF UAV FORENSIC LITERATURE (2020–2025)

Author & Year	Study Focus / Platform	Evidence Sources	Methods / Approach	Uncertainty Treatment	Confidence Quantification	Key Limitations
(Zhao et al., 2024) [9]	DJI Mavic 2 Pro forensic analysis	Drone telemetry logs, mobile artefacts	Artefact extraction, structured log parsing	Not explicitly addressed	No	Platform-specific focus
(Lee et al., 2023) [10]	DJI remote controller forensic analysis	Controller logs, pairing data	Controller artefact examination	Limited discussion	No	Limited multi-source integration
(Alotaibi et al., 2023) [11]	Conceptual UAV forensic investigation model	General UAV artefacts	Investigation framework modelling	Conceptual treatment	No	Limited empirical validation
(Studiawan et al., 2023) [12]	UAV forensic survey study	Multi-source UAV evidence	Literature classification and analysis	Minimal discussion	No	Survey-based study
(Halim & Luthfi, 2025) ,[13]	UAV flight data forensic case study	Flight telemetry logs	Static and dynamic forensic analysis	Limited treatment	No	Application-specific validation
(Tombari Sibe & Bekom, 2025) ,[14]	DJI Phantom forensic investigation	UAV internal logs	Technical case study analysis	Not explicitly addressed	No	Single platform focus
(Salamh et al., 2021),[15]	Evidence traceability analysis	Static and live UAV artefacts	Comparative forensic analysis	Partial discussion	No	Earlier UAV ecosystem
(Almusayli et al., 2024) , [16]	Digital twin forensic reconstruction	Telemetry + simulation data	Digital twin modelling approach	Partial discussion	No	Simulation dependency
(Alhasan et al., 2025),[17]	Metamodel-based forensic review	Multi-source UAV evidence	Systematic literature review	Conceptual discussion	No	Limited operational validation
(Mohammed et al., 2025),[18]	UAV cybersecurity forensic readiness	Operational UAV data streams	Security + forensic readiness framework	Partial discussion	No	Security-oriented emphasis
(Thantilage et al., 2025),19]	Law enforcement drone forensics	Logs, encrypted UAV data	Operational forensic investigation	Not explicitly addressed	No	Legal/privacy constraints
(Viswanathan & Baig, 2020),[20]	Drone forensic tools study	Tool-generated artefacts	Tool evaluation study	Minimal discussion	No	Older tool ecosystem
(Ankit et al., 2025) ,[21]	Multi-source forensic extraction case study	Chip-off, SD card, controller artefacts	Data extraction and analysis	Limited treatment	No	Platform-specific validation
(Nieszporek et al., 2026)[22]	AI-based UAV forensic identification	Mobile–UAV telemetry	Transformer-based modelling	Partial discussion	No	Emerging research stage
This Work	Multi-layer UAV forensic framework	Chip-off memory + Flight logs + Mobile artefacts + Wireless traces	Physics-based reconstruction + Temporal alignment + Evidence fusion	Explicit reliability weighting	Yes (Forensic Confidence Index)	Single case validation (future expansion planned)

III. Theoretical Foundation of UAV Forensic Inference

When treated as a purely procedural matter, digital forensic science may degenerate into a repertoire of extraction methods that lack explanatory or even inferential coherence. This danger is especially urgent in UAV research, as heterogeneous information sources, unstable storage devices, and distributed control systems make it harder to apply conventional concepts of evidence persistence and attribution. A conceptually grounded framework is therefore necessary to advance UAV forensics to the next level of technical analysis in forensic science before the court.

This is based on the Exchange Principle of Locard, but redefined for the digital and cyber-physical spaces. In UAV flights, each flight triggers cross-turning tracks across several layers: memory registers embedded in the flight, removable storage, accompanying mobile devices, and wireless communication channels. These exchanges are neither homogeneous nor equally persistent; they fluctuate, varying in volatility, granularity, and resistance to manipulation. To achieve principled evidence integration, it is essential to identify and institutionalize this asymmetric exchange of trace [23].

It should also be noted that forensic reliability and forensic certainty should be critically distinguished. The reliability is the subject of trustworthiness of some artefact under specified circumstances of acquisition, whereas the certainty suggests an unconditional conjecture that can hardly be justified by digital evidence. Modern forensic science is more often dismissing pronouncements of certainty in favor of probabilistic or confidence-bounded conclusions [24]. An example of this is UAV data, which is susceptible to sensor noise, timestamp drift, packet loss, and partial overwriting.

Therefore, confidence modelling is not a choice in UAV forensics; it is a methodological requirement. Courts and expert review panels are increasingly demanding that investigators not only state what evidence points to, but also the degree of strength the evidence has for a particular inference and the conditions under which it is made. Without direct measures of confidence, UAV forensic determinations are prone to admissibility challenges.

IV. Proposed Multi-Layer UAV Forensic Framework

A. Multi-Layer Evidence Architecture

To put the above theoretical principles into practice, a multi-layer forensic architecture is proposed. The framework clearly captures UAV evidence as a stratified system, with each layer providing different levels of information, reliability properties, and volatility restrictions.

1) Layer 1: Physical Memory (Chip-off)

This layer comprises raw non-volatile memory extracted directly from the UAV's onboard storage via chip-off procedures. It provides the best evidentiary persistence and resistance to post-incident contamination and must be acquired by invasive means and with sophisticated laboratory controls. There is high reliability and low volatility.

2) Layer 2: Logical Logs (Internal/SD Storage)

The second layer comprises flight logs, configuration files, and cached telemetry on internal flash disks or removable SD cards. These artefacts provide valuable, well-organized records of operations, but can be obsolete, overwritten, or formatted by their users. The reliability is moderate to high, depending on the time of acquisition.

3) Layer 3: Companion Device Artefacts

UAV control mobile apps produce high-context data, such as coordinated timestamps, user feedback, and stalled flight data. Although these artefacts are very informative, they are subject to the operating system's abstraction and update cycles, which create interpretive uncertainty.

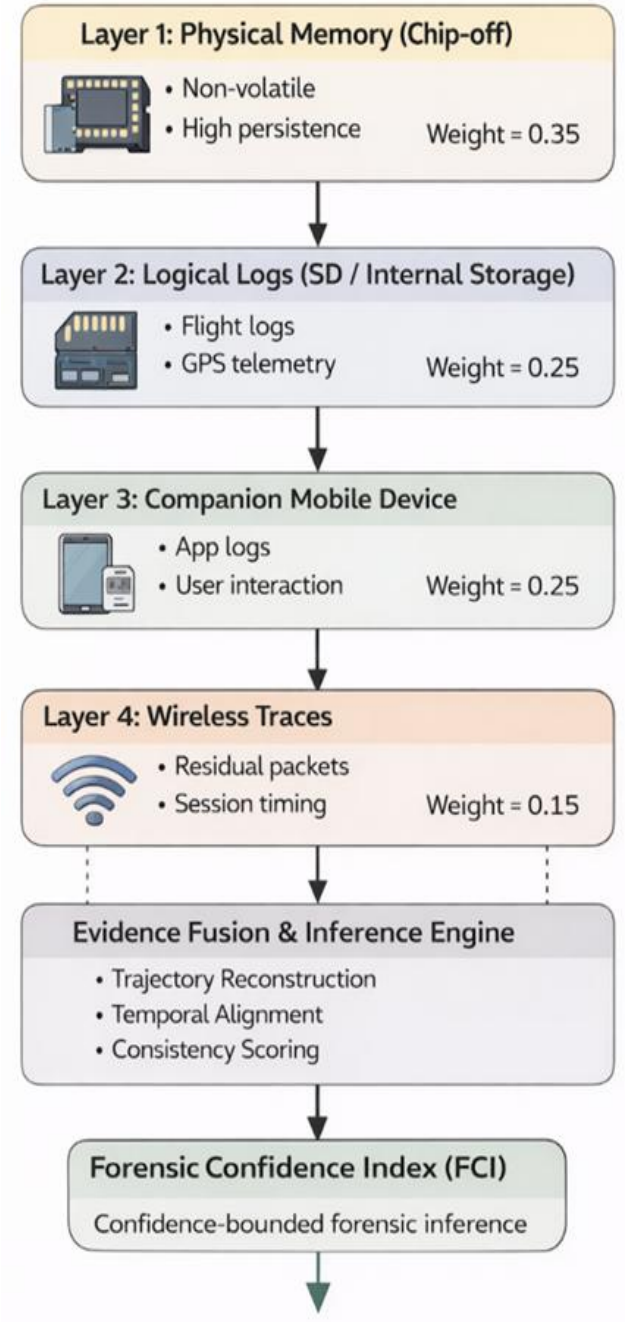

Fig. 1. Multi-layer UAV forensic evidence architecture.

4) Wireless traces: The uppermost layer comprises Wi-Fi, RF, and telemetry transmissions intercepted by access points or monitoring systems. Although partial, these transmissions provide autonomous support for UAV activity and time sequencing. This multi-layered architecture helps provide principled evidence fusion while maintaining source-specific reliability differences.

The general layout of the proposed forensic methodology is shown in Fig. 1, which models UAV evidence as a stratified, reliability-weighted system rather than a flat set of artefacts. The figure shows four forensic layers, each with distinct persistence and trust attributes: physical memory, logical logs, companion device artefacts, and wireless traces. These layers have different persistence and trust properties that are downstream of the inference process.

B. Algorithm 1: Physics-Based Flight Path Reconstruction

Reconstruction of flight paths has been a fundamental inference problem in UAV forensics. This work uses a physics-based, vendor-neutral visualization model rather than vendor-specific tools, ensuring reproducibility and cross-platform applicability.

Given sequential GPS coordinates (ϕi,λi), the geodesic distance between consecutive points is computed using the Haversine formula:

$$d = 2r\arcsin\left(\sqrt{\sin^2\left(\frac{\phi_{i+1}-\phi_i}{2}\right)+\cos(\phi_i)\cos(\phi_{i+1})\sin^2\left(\frac{\lambda_{i+1}-\lambda_i}{2}\right)}\right)$$

where,

- R= Earth radius
- ϕ= latitude
- λ= longitude

Velocity and acceleration are subsequently derived as:

$$v_i = \frac{d_i}{\Delta t_i}$$

$$a_i = \frac{v_{i+1}-v_i}{\Delta t_i}$$

where,

- d_i= distance between consecutive trajectory points
- Δt_i= time interval between successive timestamps
- v_i= velocity at the i-th interval
- a_i= acceleration derived from velocity changes

It is a formulation that allows physically implausible maneuvers to be detected, missing segments to be interpolated, and consistency checking across layers of evidence to be performed. Since the model is not based on proprietary log semantics but on the foundations of basic kinematics, it applies to UAV makers and firmware releases. Algorithm 1 presents the trajectory reconstruction.

Algorithm 1: **Trajectory Reconstruction**

GPS coordinates, timestamps

```
Compute
While (consecutive GPS points exist) do
    For (each consecutive GPS point pair) do
    Update
        Compute velocity using distance and time difference
        Compute acceleration from consecutive velocities
            If (physical plausibility condition satisfied) then
                Search
    End         End
    End
```

C. Algorithm 2: Cross-Device Temporal Alignment

Temporal congruence among heterogeneous devices remains a persistent challenge in UAV forensic investigations, particularly when correlating drone telemetry with artefacts from companion mobile devices. To address this issue, a formal synchronization model is adopted to provide structured and defensible temporal alignment.

For any event i logged on the UAV and event j recorded on the companion device, the temporal discrepancy is defined as:

$$\Delta t_{ij} = | t_i^{\text{drone}} - t_j^{\text{mobile}} |$$

To compensate for clock drift, logging latency, acquisition resolution differences, and communication delays, a synchronization tolerance parameter $\varepsilon$is introduced. Clock drift may arise from hardware timing inaccuracies, firmware offsets, or environmental conditions. Although explicit drift estimation is beyond the scope of the present study, the tolerance parameter accommodates moderate drift effects while maintaining practical forensic applicability. Future work may incorporate formal drift estimation techniques to enhance alignment precision.

False temporal alignment may occur when unrelated events fall within the tolerance window. To reduce this risk, temporal correlation is interpreted alongside contextual evidence such as flight telemetry consistency, operator interactions, and communication traces rather than relying solely on timestamp proximity.

Synchronization uncertainty is inherent in multi-device forensic investigations due to logging latency, sampling resolution, and transmission delays. The proposed tolerance-based alignment model provides a transparent mechanism for acknowledging such uncertainty while preserving

interpretability in forensic reporting. Future work will explore probabilistic synchronization models to improve robustness.

Events are considered temporally consistent when:

$$\Delta t_{ij} \leq \varepsilon$$

where,

- t_i^{drone}= UAV timestamp
- t_j^{mobile}= mobile device timestamp
- ε= synchronization tolerance

This parameterized tolerance model replaces ad hoc time matching with a more defensible alignment strategy, enabling investigators to justify synchronization decisions, quantify temporal uncertainty, and explicitly report assumptions in forensic analysis and expert testimony. Consequently, the framework helps strengthen evidentiary linkage between operator actions, device artefacts, and observed UAV behavior while addressing a methodological gap identified in prior UAV forensic research.

V. Forensic Uncertainty and Confidence Modeling

Conclusions in digital forensics that fail to acknowledge uncertainty implicitly exaggerate the strength of the evidence and, in an adversarial context, compromise their own integrity. The issue is intensified in UAV studies, where evidence is found in heterogeneous subsystems that operate under different time, physical, and operational factors. This means that uncertainty modelling and expressing confidence are not supportive additions but fundamental needs of court-facing UAV forensic science.

A. Evidence Reliability Weighting

The evidence sources in the proposed framework do not receive epistemic equivalence. Instead, each layer gets a reliability weight indicating three forensic dimensions: data persistence, user manipulation, and integrity during acquisition. These weights are not chosen unnecessarily, as they are based on the principles of digital forensic reliability established, known to date [25], and reflect empirical practice that has been reported in the literature of UAV and mobile forensics [26], [27].

The weight of physical chip-off memory is the highest because it is non-volatile and not subject to change after the event, though it is acquired invasively. So logical flight logs, which are stored on internal or removable media, are structured data on operational data but can be deleted or overwritten. Artefacts of companion mobile devices are highly detailed contextual links that are mediated by operating system abstractions and application-layer conversions. Wireless traces, although useful in corroboration, are naturally discontinuous and volatile over time [28].

The explicit weighting of these layers formalizes what is often informal in expert reasoning, thereby enhancing transparency, reproducibility, and defensibility. Extracted evidence sources are not equally forensically reliable due to variability in persistence, manipulation vulnerability, and integrity of acquisition across the ecosystem of UAVs. The weights of reliability that are attributed to each evidentiary layer and applied in this study are captured in a table in the form of Table II.

TABLE II. Evidence Reliability and Weight Assignment

Evidence Layer	Forensic Characteristics	Assigned Weight
Physical memory (chip-off)	Non-volatile, low manipulability, high persistence	0.35
Logical logs (SD/internal)	Structured records, moderate volatility	0.25
Companion mobile device	Context-rich, OS-mediated, moderate uncertainty	0.25
Wireless traces	Volatile, fragmentary, corroborative	0.15

The evidentiary weights are based on forensic reliability factors such as data persistence, susceptibility to manipulation, and acquisition integrity. Physical memory artefacts receive higher weights due to their non-volatile nature, while wireless traces are assigned lower weights because of their volatility.

B. Forensic Confidence Index (FCI) – Novel Contribution

To operationalize uncertainty-sensitive inference, the study proposes a Forensic Confidence Index (FCI), a scalar measure intended to convey the cumulative viability of evidentiary support for a particular forensic statement. The FCI is defined as:

$$\text{FCI} = \sum_{i=1}^{n} w_i C_i$$

where,

- w_i= reliability weight of the i-th evidence layer
- C_i= normalized consistency score (0–1)
- n= number of evidence layers

The proposed Forensic Confidence Index represents a methodological framework rather than a fully statistically validated model. Future studies will focus on empirical calibration using larger UAV forensic datasets.

Where w_i represents the reliability weight of the i -th evidence layer, and $C_i$denotes the normalized consistency score (ranging from 0 to 1) reflecting the internal coherence and cross-layer corroboration of that evidence layer.

The thresholds of the interpretation are established to embrace forensic reporting and expert testimony:

FCI ≥ 0.80: Strong forensic support

0.60 ≤ FCI < 0.80: Moderate support with acknowledged uncertainty

FCI < 0.60: Weak or insufficient support

The FCI threshold values are heuristic and intended to support interpretive guidance rather than absolute probabilistic certainty. Further empirical validation will refine these thresholds.

More importantly, the FCI does not purport to know. Instead, it offers a clear, quantitative expression of confidence that can be scrutinized, challenged, and contextualized - a requirement also emphasized in digital forensic admissibility criteria. An overview of UAV forensic research published in 2020-2025 shows that no similar tool exists to articulate attribution confidence using a combination of evidence types, making this contribution both innovative and needed.

The mathematical calculations behind the Forensic Confidence Index are illustrated in Fig. 2, which shows how heterogeneous evidence inputs are transformed by weighting reliability and scoring consistency, and then aggregated into a single confidence-constrained measure.

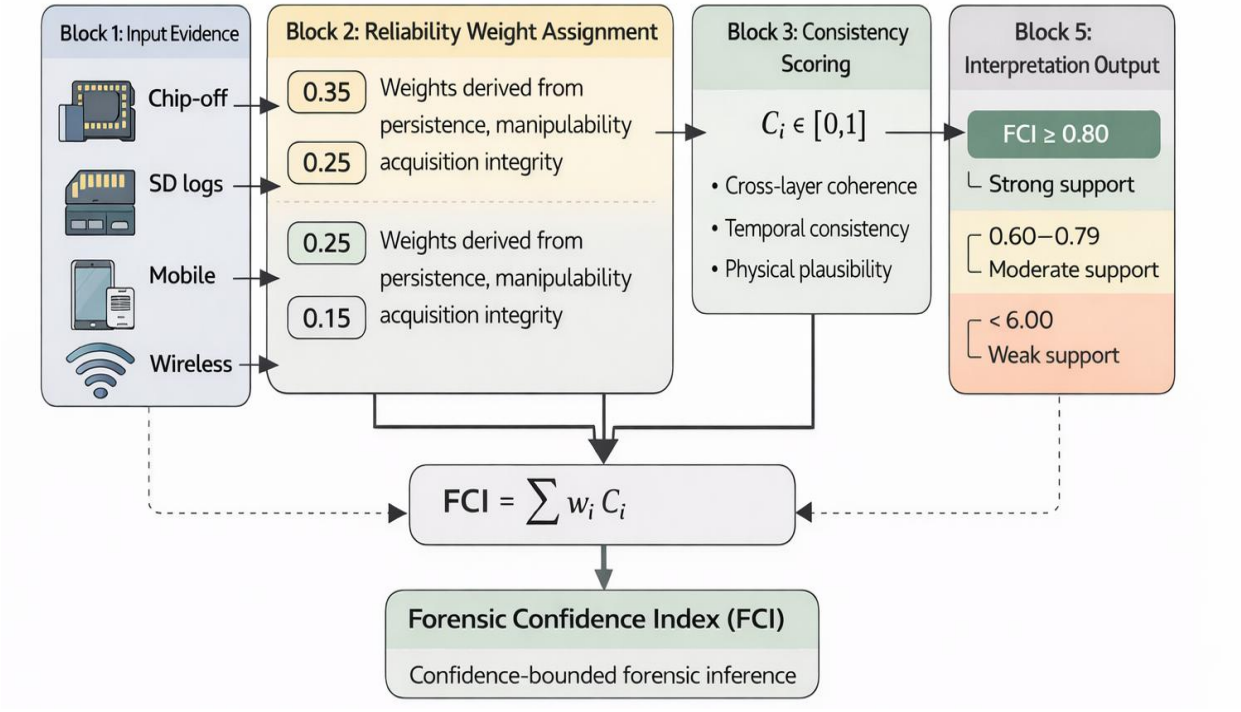

Fig. 2. Forensic Confidence Index computation flow.

VI. Case Study: Yuneec Typhoon Q500 4K (Validation Only)

Forensic science case studies are confirmatory, not creative: they show that a proposed set of concepts can work within real-world constraints. Although the validation focuses on a single UAV platform, this case study serves as a proof-of-concept for the proposed framework under realistic forensic conditions. In emerging forensic domains, initial validation often relies on representative case studies before broader multi-platform evaluation becomes feasible. Accordingly, the Yuneec Typhoon Q500 4K is used as a validation platform for the multi-layer forensic framework, algorithms, and confidence modelling methodology presented earlier.

The inspected UAV was recovered after it was suspected of being used in an unauthorized surveillance operation. The acquisition process was forensically sound, including invasive chip-off acquisition of onboard flash memory, logical acquisition of SD card flight logs, forensic imaging of the companion device, which was also based on Android, and preservation of residual wireless communication artefacts on the local access point. Write-blocked workflows were used for all acquisitions, and the integrity of the evidence was verified through cryptographic hashing of the message.

The artefacts across the four layers of evidence differed in persistence, granularity, and internal coherence. Physical memory provided low-level configuration residues and partial flight buffers that were difficult for the user to erase. Logical logs provided formatted GPS telemetry and timed flight events. Artifacts from companion devices provided application-level sync points and operator touchpoint metadata, whereas wireless traces provided corroborative time anchors at takeoff and landing. More importantly, none of the layers was considered dispositive; the value of the evidence appeared only in the form of systematic composition.

The reconstructed flight path algorithm produced a continuous three-dimensional path within the physical limits of the Q500 platform, and discrepancies between the drone and mobile timestamps were addressed by time-matching within the specified synchronization error. Using the Forensic Confidence Index (FCI), a composite score indicating strong evidentiary support but not absolute confidence was obtained.

The case study focuses on implementing the proposed framework on real forensic artefacts recovered from a Yuneec Typhoon Q500 4K UAV. Table III provides a summary of all recovered artefacts, their provenience, and the confidence measures.

TABLE III. EXTRACTED FORENSIC ARTEFACTS SUMMARY

Source	Artefacts Identified	Count	Confidence Contribution
Chip-off Memory	Configuration remnants, partial buffers	0.35	High
SD card logs	GPS points, timestamps, flight states	0.25	Moderate - High
Companion mobile device	App logs, user actions, sync markers	0.25	Moderate
Wireless traces	Connection timestamps, session IDs	0.15	Low - Moderate

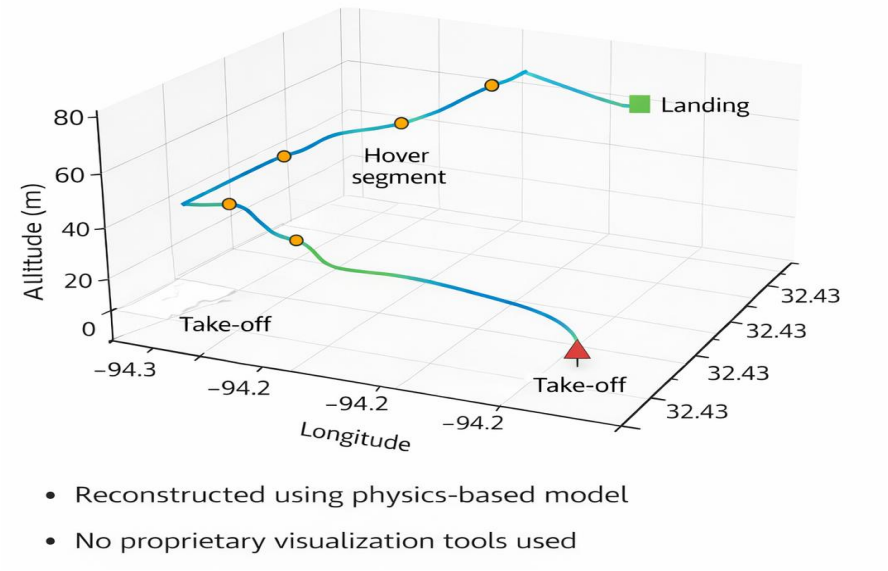

Fig. 3. 3D Flight path reconstruction of yuneec typhoon Q500 4K.

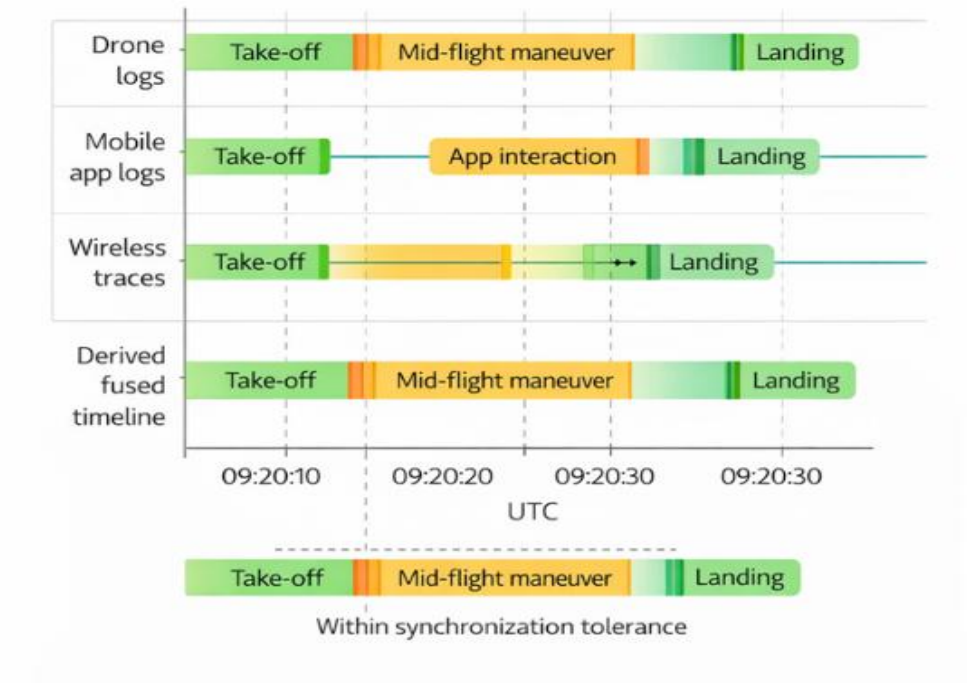

Fig. 4. Cross-device evidence correlation timeline.

The recovered flight path, based on telemetry from the SD card, is plotted in Fig. 3 and shows a physically possible three-dimensional flight path that aligns with the reported take-off, maneuvering, and landing events.

Temporal correspondence between drone logs, mobile application artefacts, and wireless traces is shown in Fig. 4, which presents a coherent timeline extracted within specified synchronization margins.

VII. Discussion: Comparative and Theoretical Implications

The significance of the present study's findings extends beyond artefact retrieval to their implications for the conceptualization, integration, and interpretation of UAV forensic evidence. Compared with previously reported UAV forensic case studies involving DJI and Yuneec platforms, which largely emphasize artefact extraction and platform-specific analysis, the proposed framework explicitly integrates multi-layer evidence fusion, uncertainty modelling, and confidence quantification. This methodological shift enables more transparent forensic inference while maintaining compatibility with established UAV forensic workflows. Earlier studies have demonstrated successful access to forensic artefacts; however, the evidentiary strength often remained implicit and dependent on investigator interpretation rather than structured inference models.

The proposed framework advances UAV forensic investigation along three complementary dimensions. First, physics-based trajectory validation replaces purely descriptive reconstruction, reducing reliance on proprietary visualization tools and improving reproducibility. Second, structured cross-device temporal alignment provides a systematic mechanism for addressing timestamp inconsistencies frequently encountered in forensic investigations and litigation contexts. Third, the explicit incorporation of uncertainty management through reliability weighting and the Forensic Confidence Index (FCI) introduces a quantified representation of evidentiary confidence that has been largely absent from prior UAV forensic literature.

From an interpretive standpoint, the FCI results illustrate how heterogeneous evidence sources contribute differently to overall forensic confidence. More persistent artefacts, such as onboard memory and structured flight logs, typically provide stronger evidentiary stability, whereas volatile wireless traces act primarily as corroborative indicators. This structured integration enhances evidentiary coherence compared with single-source forensic approaches while maintaining transparency regarding uncertainty.

Theoretically, these findings reinforce the applicability of the digital Locard's exchange principle within cyber-physical forensic environments and clarify the distinction between evidentiary certainty and inferential confidence. Rather than asserting deterministic conclusions, the framework promotes calibrated confidence reporting, an approach increasingly recognized as essential for scientific credibility and legal defensibility in forensic science.

More broadly, the framework suggests a transition in UAV forensic practice from artefact-oriented reporting towards inference-oriented reasoning. Such a transition supports improved transparency, reproducibility, and judicial admissibility while aligning UAV forensic methodologies with evolving forensic science standards. Sensitivity considerations indicate that moderate variations in evidentiary weights do not substantially alter overall confidence classification, suggesting preliminary robustness of the framework. Nevertheless, comprehensive quantitative sensitivity analysis and multi-platform empirical validation remain important directions for future work.

VIII. Generalization, Admissibility, and Practical Deployment

To have long-term value, a UAV forensic framework should not be confined to a single platform, while remaining in line with operational and legal limitations. Even though its validation is performed with the Yuneec Typhoon Q500 4K, the proposed framework is deliberately manufacturer-agnostic. The fact that its use of physics-based trajectory reconstruction, abstracted temporal alignment, and evidence-layer weighting is directly applicable to the ecosystems of DJI, Parrot, and Autel UAVs, despite their proprietary log formats or telemetry encodings, is possible [29]. More to the point, the framework is independent of tools. The algorithms are applied to normalized artefact representations rather than vendor-specific parsers, allowing the investigator to combine commercial, open-source, or lab-written tools without modifying the inferential logic. This design option directly reinforces reproducibility and overcomes tool-bias challenges, which are increasingly contentious in forensic admissibility trials.

Legally, the framework corresponds to the principles of reliability used in Daubert-style tests: methods are testable, sources of error are recognized through uncertainty modelling, and inferential steps are transparent and reproducible. Chain-of-custody integrity is maintained by supporting standard forensic acquisition processes and by hash-verified handling of evidence. Conclusions derived from the framework can therefore be expressed as expert opinions with confidence limits, rather than unprovable claims.

IX. Limitations and Future Directions

The strengths notwithstanding, the framework suggested has some limitations. Streaming encrypted telemetry and firmware seals might curtail access to artefacts on newer UAV systems, diminishing the degree of multi-layer evidence integration. Also, the current implementation of wireless trace analysis relies on residual or post-event data; real-time software-defined radio (SDR) capture would improve time resolution but raise logistical and legal issues. The current FCI formulation relies on theoretically grounded weight assignments and requires broader empirical validation across diverse UAV forensic scenarios. Future work will extend validation across multiple UAV platforms, including DJI, Parrot, and Autel ecosystems, to evaluate generalizability and robustness under diverse operational conditions.

To address the problem of time-dependent updating of confidence scores as new evidence is found, future work may generalize the Forensic Confidence Index using probabilistic or Bayesian machine learning models that dynamically update confidence scores as new evidence becomes available. These extensions, though, should be rigorously scrutinized to maintain their interpretability and to remain non-opaque in their explanations before the court.

X. Conclusion

This study advances UAV forensic science by shifting the focus from artefact-centric examination toward confidence-aware forensic inference. A theoretically grounded multi-layer framework was proposed that integrates physics-based trajectory reconstruction, structured cross-device temporal

alignment, and explicit uncertainty modelling. The introduction of the Forensic Confidence Index (FCI) provides a systematic mechanism for expressing evidentiary strength without overstating certainty, thereby supporting transparent and defensible forensic reporting.

The findings demonstrate that multi-layer evidence integration improves evidentiary coherence and interpretability compared with purely descriptive artefact analysis. This approach has practical implications for enhancing transparency, reproducibility, and legal defensibility in UAV forensic investigations while aligning forensic practice with emerging scientific and judicial expectations.

However, validation in the present study is based on a single UAV platform (Yuneec Typhoon Q500 4K), and broader empirical evaluation across diverse UAV ecosystems remains necessary to strengthen generalizability. Despite this limitation, the framework establishes a methodological foundation for structured confidence-aware inference in cyber-physical forensic environments.

Future work will focus on multi-platform empirical validation, refinement of reliability weight assignments, and quantitative sensitivity analysis to further strengthen confidence assessment in UAV forensic investigations.

REFERENCES

[1] D. Y. Kao, M. C. Chen, W. Y. Wu, J. S. Lin, C. H. Chen, and F. Tsai, "Drone forensic investigation: DJI spark drone as a case study," Procedia Comput. Sci., vol. 159, pp. 1890–1899, 2019, doi: 10.1016/J.PROCS.2019.09.361.

[2] "Unmanned Aerial Vehicle Forensic Investigation Process: Dji Phantom 3 Drone As A Case Study | Request PDF." Accessed: Jan. 24, 2026. [Online]. Available: https://www.researchgate.net/publication/324745129_Unmanned_Aerial_Vehicle_Forensic_Investigation_Process_Dji_Phantom_3_Drone_As_A_Case_Study

[3] G. De La Torre, P. Rad, and K. K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," Future Generation Computer Systems, vol. 108, pp. 1092–1111, Jul. 2020, doi: 10.1016/J.FUTURE.2017.12.041.

[4] D. Kovar, "Who We Are."

[5] "Gartner Says Almost 3 Million Personal and Commercial Drones Will Be Shipped in 2017." Accessed: Jan. 24, 2026. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-09-gartner-says-almost-3-million-personal-and-commercial-drones-will-be-shipped-in-2017

[6] K. Chávez and O. Swed, "The proliferation of drones to violent nonstate actors," Defence Studies, vol. 21, no. 1, pp. 1–24, Jan. 2021, doi: 10.1080/14702436.2020.1848426;WGROUP:STRING:PUBLICATION.

[7] N. Riya Rajendran, G. Hemi, M. Dipak Kumar, P. Behumiraj, and P. Ankita, "Drone Forensics," Advanced Techniques and Applications of Cybersecurity and Forensics, pp. 99–123, Jul. 2024, doi: 10.1201/9781003386926-6.

[8] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," Digit. Investig., vol. 16, pp. 1–11, Mar. 2016, doi: 10.1016/J.DIIN.2015.11.002.

[9] Z. Zhao, Y. Wang, and G. Liao, "Digital Forensic Research for Analyzing Drone and Mobile Device: Focusing on DJI Mavic 2 Pro," Drones 2024, Vol. 8, vol. 8, no. 7, Jun. 2024, doi: 10.3390/drones8070281.

[10] S. Lee, H. Seo, and D. Kim, "Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller," Sensors (Basel)., vol. 23, no. 21, p. 8934, Nov. 2023, doi: 10.3390/s23218934.

[11] F. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field," Engineering, Technology & Applied Science Research, vol. 13, no. 5, pp. 11608–11615, Oct. 2023, doi: 10.48084/etasr.6195.

[12] H. Studiawan, G. Grispos, and K. K. R. Choo, "Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed," Comput. Secur., vol. 132, no. 13, p. 103340, Sep. 2023, doi: 10.1016/j.cose.2023.103340.

[13] M. Y. Halim and A. Luthfi, "Digital Forensic Analysis of UAV Flight Data Using Static and Dynamic Methods in Coal Mining Area," Journal of Information Systems and Informatics, vol. 7, no. 2, pp. 1042–1060, Jun. 2025, doi: 10.51519/journalisi.v7i2.1061.

[14] R. Tombari Sibe and D. Bekom, "Digital Forensic Investigation of an Unmanned Aerial Vehicle (UAV): A Technical Case Study of a DJI Phantom III Professional Drone," Journal of Cybersecurity and Information Management, vol. 15, no. 1, pp. 197–210, 2025, doi: 10.54216/JCIM.150115.

[15] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, "A comparative uav forensic analysis: Static and live digital evidence traceability challenges," Drones, vol. 5, no. 2, Jun. 2021, doi: 10.3390/drones5020042.

[16] A. Almusayli, T. Zia, and E. U. H. Qazi, "Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology," Technologies 2024, Vol. 12, vol. 12, no. 1, Jan. 2024, doi: 10.3390/technologies12010011.

[17] S. A. M. Alhasan, S. H. Othman, and A. Al-Dhaqm, "Metamodeling-Based Drone Forensics Investigation: A Systematic Literature Review," International Journal of Safety and Security Engineering, vol. 15, no. 1, pp. 1–12, Jan. 2025, doi: 10.18280/ijsse.150101.

[18] U. M. Mohammed et al., "Cyber threat in drone systems: bridging real-time security, legal admissibility, and digital forensic solution readiness," Frontiers in Communications and Networks, vol. 6, p. 1661928, Sep. 2025, doi: 10.3389/frcmn.2025.1661928.

[19] R. D. Thantilage, G. Buttner, and R. Genoe, "Drone forensics in law enforcement: Assessing utilisation, challenges, and emerging necessities," Forensic Science International: Digital Investigation, vol. 55, no. 13, p. 302003, Dec. 2025, doi: 10.1016/j.fsidi.2025.302003.

[20] S. Viswanathan and Z. Baig, "Digital Forensics for Drones: A Study of Tools and Techniques," Communications in Computer and Information Science, vol. 1338, pp. 29–41, 2020, doi: 10.1007/978-981-33-4706-9_3.

[21] Ankit, T. Kumar, and H. K. Singhal, "Forensics Case studies – Extraction of deleted and live data from DJI Agras MG 1s Drone Through Chip-off, Internal SD Card and Controller Chip-off Extraction.," International Journal of Innovative Research in Technology, vol. 11, no. 8, pp. 1628–1636, 2025, Accessed: Feb. 13, 2026. [Online]. Available: https://ijirt.org/article?manuscript=172020

[22] K. Nieszporek, J. Bernacki, K. A. P. Costa, Q. Ke, and W. Wei, "UAV Forensics: Transformer-Based Identification of Mobile Devices for Drone Piloting," Lecture Notes in Computer Science, vol. 15949 LNCS, pp. 355–363, 2026, doi: 10.1007/978-3-032-03708-4_29.

[23] E. Mantas and C. Patsakis, "Who watches the new watchmen? The challenges for drone digital forensics investigations," Array, vol. 14, p. 100135, Jul. 2022, doi: 10.1016/J.ARRAY.2022.100135.

[24] R. Tombari Sibe and D. Bekom, "Digital Forensic Investigation of an Unmanned Aerial Vehicle (UAV): A Technical Case Study of a DJI Phantom III Professional Drone," Journal of Cybersecurity and Information Management, vol. 15, no. 1, pp. 197–210, 2025, doi: 10.54216/JCIM.150115.

[25] F. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field," Engineering, Technology & Applied Science Research, vol. 13, no. 5, pp. 11608–11615, Oct. 2023, doi: 10.48084/ETASR.6195.

[26] H. Studiawan, G. Grispos, and K. K. R. Choo, "Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed," Comput. Secur., vol. 132, Sep. 2023, doi: 10.1016/J.COSE.2023.103340.

[27] A. Taylor, "A Digital Forensics Case Study of the DJI Mini 3 Pro and DJI RC," Sep. 2023, Accessed: Jan. 24, 2026. [Online]. Available: https://arxiv.org/pdf/2309.10487

[28] S. Lee, H. Seo, and D. Kim, "Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller," Sensors 2023, Vol. 23, vol. 23, no. 21, Nov. 2023, doi: 10.3390/S23218934.

[29] D. Lee and W. Kang, "Drone forensics redefined: Integrating live, digital, and non-digital evidence acquisition systems," Forensic Sci. Int., vol. 11, p. 100635, Dec. 2025, doi: 10.1016/J.FSISYN.2025.100635.