Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Addressing Inadequate Forensic Training and Resources for Law Enforcement National Strategy in Drone Based Investigations

Syed Usman Jamil*[1], M. A. Rahman[2], M. Arif Khan[3], Muhammad Adeel[4] and Muhammad Ali Paracha[5]

[1]School of Computing, Mathematics and Engineering, Charles Sturt University, Wagga Wagga, NSW 2650, Australia
[2]College of Computer and Cyber Sciences, University of Prince Mugrin, Madina, KSA
[3]School of Computing, Mathematics and Engineering, Charles Sturt University, Wagga Wagga, NSW 2650, Australia
[4]University of North Texas at Dallas, Dallas, TX, USA
[5]CDC, Melbourne, Vic, Australia.

Received 27 Nov. 2025; Accepted 27 Dec. 2025; Available Online 31 Dec. 2025

Abstract

The rapid proliferation of unmanned aerial vehicles (UAVs) has introduced new complexities to forensic investigations, exposing gaps in training, protocols, and scalable resources particularly for smaller or remote jurisdictions. This study proposes a national strategy that unifies three pillars: (i) operational readiness through tiered certification, microlearning, rapid deployment kits, and standardized procedures; (ii) equitable regional support via shared laboratories, knowledge portals, and capability assessments; and (iii) workforce development via diversified recruitment, apprenticeships, and retention incentives. The framework synthesizes evidence from recent initiatives and commercially available toolchains to offer a scalable, standards-aligned approach for securing, processing, and presenting drone-derived digital evidence. Emphasis is placed on institutional learning, accreditation harmoniza-tion, and mechanisms for sustaining expertise. The strategy is intended as a practical, evidence-based model to improve consistency and admissibility of drone evidence across heterogeneous agency contexts.

I. Introduction

Unmanned aerial vehicles (UAVs), commonly referred to as drones, have become increasingly prevalent across commercial, recreational, military, and criminal domains [1]. Their accessibility and versatility have enabled a wide range of activities, including package delivery, aerial photography, infrastructure monitoring, humanitarian aid, and agricultural management. However, drones have also been exploited for illicit purposes such as smuggling contraband, unauthorized surveillance, sabotage, terror-ism, and targeted attacks [2]. The integration of drones into asymmetric warfare has been particularly visible in recent conflicts such as the Russia–Ukraine war, where drone swarms have been deployed for reconnaissance, intelligence gathering, and precision strikes [3]. Similarly, cross-border tensions between India and Pakistan have included the use of drones for arms delivery and

Keywords: Digital forensics capacity building, drone forensics, forensic readiness, law enforcement training, unmanned aerial vehicle (UAV) investigation

Production and hosting by NAUSS

* Corresponding Author: Syed Usman Jamil
Email: sjamil@csu.edu.au

doi: 10.26735/UXIL7584

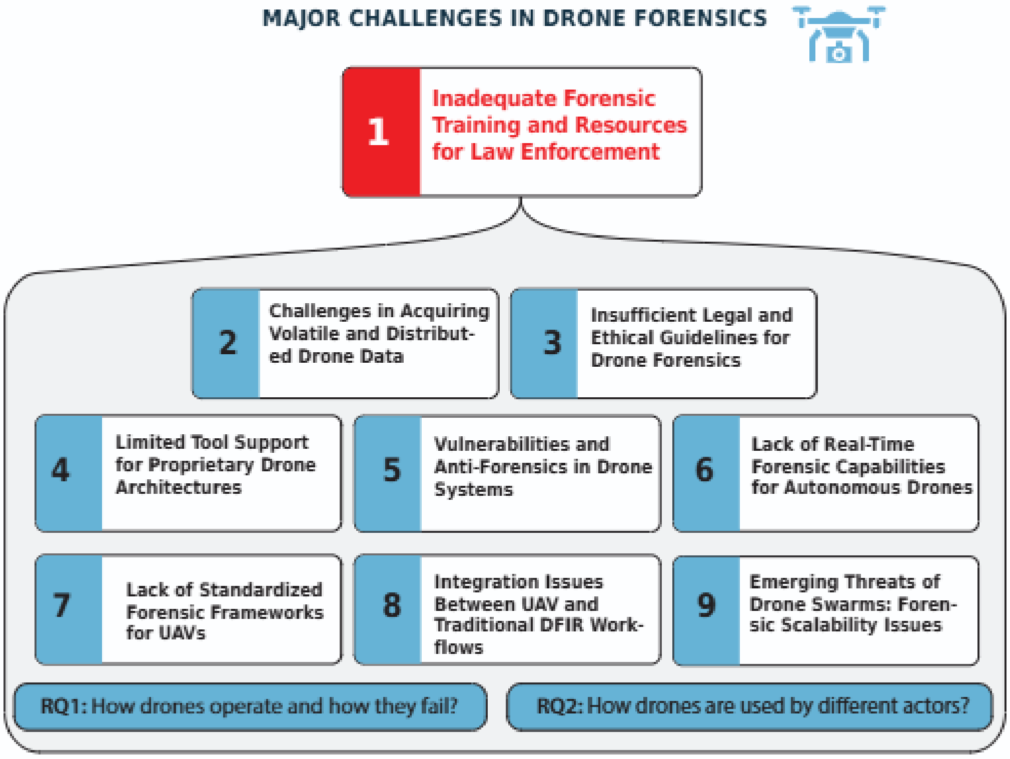
MAJOR CHALLENGES IN DRONE FORENSICS
1 Inadequate Forensic Training and Resources for Law Enforcement
2 Challenges in Acquiring Volatile and Distributed Drone Data
3 Insufficient Legal and Ethical Guidelines for Drone Forensics
4 Limited Tool Support for Proprietary Drone Architectures
5 Vulnerabilities and Anti-Forensics in Drone Systems
6 Lack of Real-Time Forensic Capabilities for Autonomous Drones
7 Lack of Standardized Forensic Frameworks for UAVs
8 Integration Issues Between UAV and Traditional DFIR Workflows
9 Emerging Threats of Drone Swarms: Forensic Scalability Issues
RQ1: How drones operate and how they fail?
RQ2: How drones are used by different actors?

Fig. 1: Summary of the major challenges affecting the reliability, scalability, and legal defensibility of drone forensic investigations.

espionage [4], while Israel and Iran have engaged in drone-based operations for surveillance and targeted engagements [5]. The dual-use nature of drones creates significant challenges for forensic investigators and legal authorities [6]. Incidents often require the collection of evidence that may be presented in domestic criminal courts, military tribunals, or even international legal forums such as the International Court of Justice [7]. The consequences of in-adequate forensic readiness are far-reaching: domestically, untrained personnel may mishandle evidence, leading to failed prosecutions and erosion of public confidence. Internationally, improperly documented evidence can un-determine accountability efforts and diminish the credibility of states seeking to prove violations of sovereignty or humanitarian law.

Despite the urgency of these challenges, there remains a substantial gap in training programs, standardized protocols, and institutional capacity for drone forensic investigation [8]. While a few universities and professional organizations [9]–[18] have begun to address this emerging field, their efforts remain fragmented and insufficient to meet the growing demand for qualified practitioners.

A. Overview of Major Challenges in Drone Forensics

Drone forensics is an emerging subfield within digital forensics, but it remains fraught with a range of critical challenges that limit its effectiveness in real-world investigations [19]. Figure 1 outlines ten major issues that collectively impact the reliability, scalability, and legal defensibility of forensic processes involving unmanned aerial vehicles (UAVs). This Figure presents a synthesized overview of key challenges in contemporary drone forensics, developed through an extensive review of academic literature, technical reports, and practitioner resources. Rather than reflecting a single study, the figure consolidates recurring gaps reported across multiple sources, capturing common limitations related to training, operational readiness, resource availability, and standardization.

The drone forensics landscape is characterized by multiple technical, operational, and legal challenges. Figure 1 presents a synthesized overview of the major challenges identified in this study. These challenges represent the authors' collective interpretation and consolidation of findings reported across diverse prior studies and practitioner sources, rather than being derived from any single reference.

Several challenges are particularly prominent, including difficulties in acquiring volatile and distributed drone data (Challenge 2), insufficient legal and ethical guidance for drone forensic investigations (Challenge 3), limited tool support for proprietary architectures (Challenge 4), are particularly prominent, including difficulties in acquiring volatile and distributed drone data (Challenge 2), insufficient legal and ethical guidance for drone forensic investigations (Challenge 3), limited tool support for proprietary drone architectures (Challenge 4), and the presence of vulnerabilities and anti-forensic mechanisms within drone systems (Challenge 5). Additional complexities arise from the lack of real-time forensic capabilities for autonomous drones (Challenge 6), the absence of standardized forensic frameworks for UAVs (Challenge 7), and integration gaps between UAV-specific forensic processes and traditional Digital Forensics and Incident Response (DFIR) workflows (Challenge 8). Emerging drone swarm operations further introduce scalability challenges in evidence acquisition and attribution (Challenge 9).

This study focuses specifically on Challenge 1: Inadequate Forensic Training and Resources for Law Enforcement, which is visually highlighted in Figure 1. Despite the increasing adoption of drones in both civilian and criminal contexts, many law enforcement agencies lack specialized training, standardized investigative procedures, and validated toolsets for effective drone forensic analysis. This limitation can delay investigative response and increase the risk of evidence mishandling or inadmissibility. To address this gap, the paper proposes a scalable and modular training framework aimed at strengthening technical, legal, and operational competencies in drone forensics.

While the present work centers on Challenge 1, the remaining challenges identified in Figure 1 are acknowledged as part of a broader research agenda for research community. These will be systematically explored in future studies to support the development of a comprehensive, standardized, and legally defensible UAV forensic framework.

B. Use-Case: Investigative Training Gaps

Regarding drone-based investigations (Figure 1), the national interest falls primarily into two key domains:

1) Technical Investigation of Drones (RQ1): This focuses on understanding how drones operate and how they fail, including:

- Analysis of drone architecture and control mechanisms
- Identification of failure modes, malfunctions, and system vulnerabilities.
- Investigation of swarm drones, including coordination, communication, and collective failure behaviours.

2) Operational Use of Drones by Entities (RQ2): This examines how drones are used by different actors, including:

- Law Enforcement Use of Drones: a) Deployment of drones for surveillance, search and rescue, border security, and public safety, b) Regulatory compliance, ethical considerations, and account-ability in drone operations.
- Criminal or Malicious Use of Drones: a) Use of drones for illegal surveillance, smuggling, re-connaissance, or attacks, b) Investigation method-ologies employed by law enforcement to identify operators, trace drone activity, and collect forensic evidences

Lets discuss it with the help of example, Figure 2 presents an investigative scenario based on Operation Night Drop [20], showing how drone-enabled crimes progress from incident to investigative failure when specialized forensics are lacking. It begins with a Drone Incident. a commercial off-the-shelf UAV approaches a restricted correctional facility and autonomously drops a payload inside the perimeter. These brief, nocturnal flights are designed to evade conventional security and visual detection.

In the second stage, Drone Misuse for Crimes, the UAV serves as a low-risk delivery platform for narcotics and contraband phones, supporting

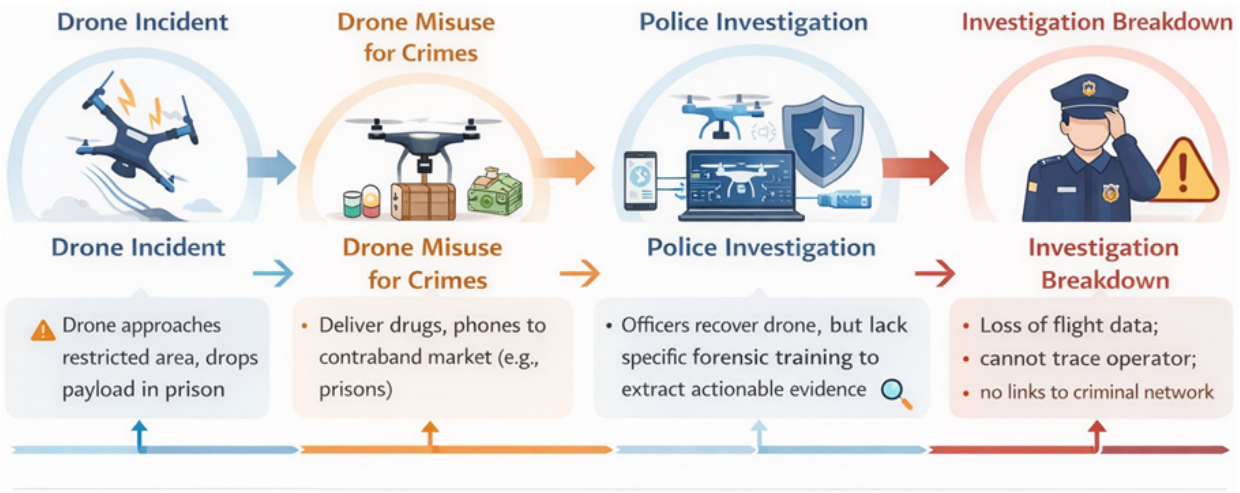
Drone Incident
Drone Misuse for Crimes
Police Investigation
Investigation Breakdown
Drone Incident
Drone Misuse for Crimes
Police Investigation
Investigation Breakdown
Drone approaches restricted area, drops payload in prison
• Deliver drugs, phones to contraband market (e.g., prisons)
• Officers recover drone, but lack specific forensic training to extract actionable evidence
• Loss of flight data;
• cannot trace operator;
• no links to criminal network

Fig. 2: Illustrative investigative flow highlighting a few of training gaps in drone-enabled crimes

organized criminal networks inside and outside prisons. As in the Night Drop indictments, cheap, disposable, and easy-to-use drones enable repeated missions with minimal operator risk.

The third stage is the Police Investigation, where officers may recover a crashed or abandoned drone or seize delivered contraband. However, as the case and diagram show, investigators often lack drone-specific forensic skills to extract usable evidence. Key artefacts volatile flight telemetry, controller pairing data, firmware logs, application data, and RF traces are frequently overlooked or lost due to delays and poor evidence triage.

This leads to the final stage, Investigation Breakdown. Even with seized physical evidence, investigators often cannot reconstruct flight paths, attribute the UAV to an operator, or link it to a wider network. Loss of ephemeral data and the absence of standardized UAV forensic procedures weaken attribution, reduce prosecutorial value, and forfeit chances to disrupt organized smuggling.

The Operation Night Drop case shows that the core issue is not missing technology, but inadequate structured forensic training and operational preparedness. This underpins Challenge 1: Inadequate Forensic Training and Resources for Law Enforcement. Addressing it requires role-specific training that integrates UAV awareness, rapid volatile data preservation, and legally robust evidence handling into routine correctional and criminal investigations. The scenario in Figure 2 thus motivates the national capability framework proposed in this study.

C. Objective of the Study

The primary objective of this study is to address the critical gap in forensic readiness, practitioner training, and resource accessibility among law enforcement agencies encountering drone-enabled criminal activity. Although drone forensics has evolved in technical sophistication, its operational adoption remains fragmented, inconsistent, and highly dependent on local capabilities. This work aims to design a unified national strategy that equips agencies of all sizes through structured training pathways, rapid deployment toolkits, standardized protocols, and equitable access to technical expertise. The proposed framework integrates modular microlearning, national certification tiers, regional support hubs, and expert assistance to establish a consistent, sustainable, and legally defensible drone forensics ecosystem. In doing so, the study seeks to transform drone forensics from an isolated technical practice into a scalable national capability that supports frontline responders, investigators, and analysts across rural, urban, remote, and coastal jurisdictions.

D. Contributions

This study makes several key contributions to the evolving domain of drone forensics:

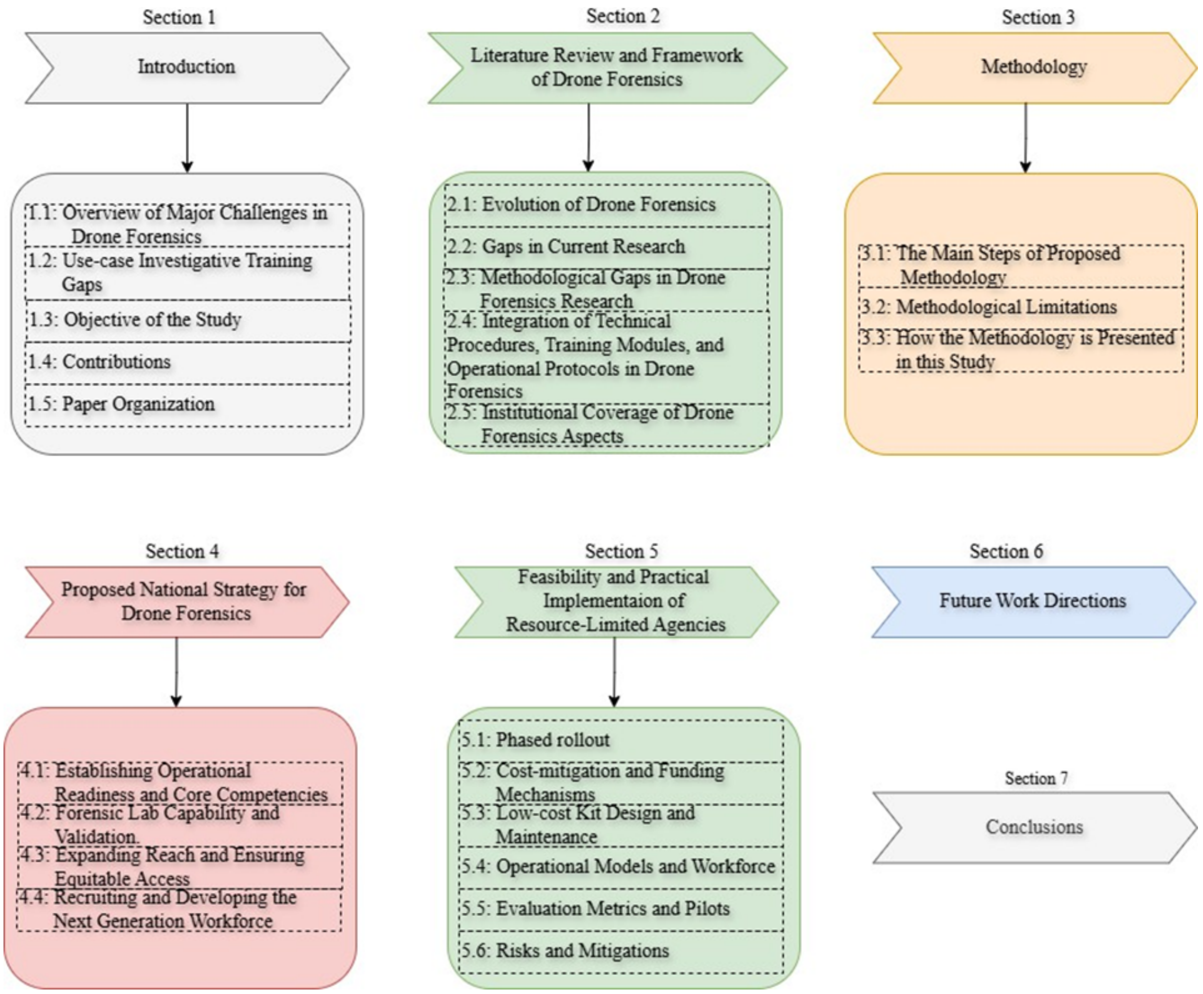
Section 1
Introduction
1.1: Overview of Major Challenges in Drone Forensics
1.2: Use-case Investigative Training Gaps
1.3: Objective of the Study
1.4: Contributions
1.5: Paper Organization
Section 2
Literature Review and Framework of Drone Forensics
2.1: Evolution of Drone Forensics
2.2: Gaps in Current Research
2.3: Methodological Gaps in Drone Forensics Research
2.4: Integration of Technical Procedures, Training Modules, and Operational Protocols in Drone Forensics
2.5: Institutional Coverage of Drone Forensics Aspects
Section 3
Methodology
3.1: The Main Steps of Proposed Methodology
3.2: Methodological Limitations
3.3: How the Methodology is Presented in this Study
Section 4
Proposed National Strategy for Drone Forensics
4.1: Establishing Operational Readiness and Core Competencies
4.2: Forensic Lab Capability and Validation
4.3: Expanding Reach and Ensuring Equitable Access
4.4: Recruiting and Developing the Next Generation Workforce
Section 5
Feasibility and Practical Implementaion of Resource-Limited Agencies
5.1: Phased rollout
5.2: Cost-mitigation and Funding Mechanisms
5.3: Low-cost Kit Design and Maintenance
5.4: Operational Models and Workforce
5.5: Evaluation Metrics and Pilots
5.6: Risks and Mitigations
Section 6
Future Work Directions
Section 7
Conclusions

Fig. 3: Paper structural flow

- Systematic Review of academic, professional and research settings in drone forensics.
- National Capability Framework: A comprehensive blueprint integrating training, operational procedures, digital evidence workflows, and expert support into a cohesive, scalable approach for law enforcement agencies.
- Tiered Certification Ecosystem: A structured path-way from foundational drone awareness to advanced forensic analysis, enabling consistent competency building regardless of agency size or resource level.
- Resource Toolkit and Mobile Infrastructure: Development of Rapid Deployment Forensics Kits, mobile applications for real-time evidence guidance, and remote extraction workflows that minimize evidence loss and improve response speed.
- Regional Drone Forensics Cells: A model for distributed forensic support through laboratory-equipped regional hubs, satellite facilities, and partnerships with state, federal, and academic institutions.
- Workforce Development Pipeline: A national talent strategy encompassing recruitment channels, academic partnerships, apprenticeships, mentorship hubs, and retention incentives to address long-term shortages in forensic specialists.
- Standardized Operating Procedures: Harmonized documentation templates, validation pathways, and chain-of-custody guidelines aligned with established forensic

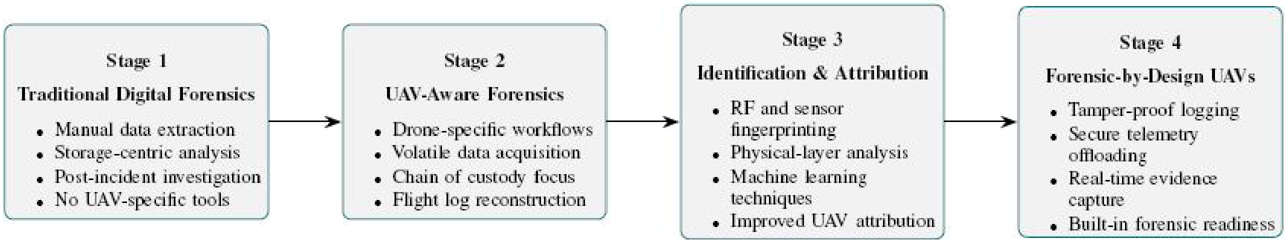
Stage 1
Traditional Digital Forensics
Manual data extraction
Storage-centric analysis
Post-incident investigation
No UAV-specific tools
Stage 2
UAV-Aware Forensics
Drone-specific workflows
Volatile data acquisition
Chain of custody focus
Flight log reconstruction
Stage 3
Identification & Attribution
RF and sensor fingerprinting
Physical-layer analysis
Machine learning techniques
Improved UAV attribution
Stage 4
Forensic-by-Design UAVs
Tamper-proof logging
Secure telemetry offloading
Real-time evidence capture
Built-in forensic readiness

Fig. 4: Evolution stages of drone forensics, illustrating the transition from traditional digital forensic practices to advanced forensic-by-design UAV frameworks.

standards to enhance cross-jurisdictional admissibility.

Collectively, these contributions offer an actionable, future-oriented framework for elevating drone forensics to a resilient, standardized, and nationally coordinated practice.

E. Paper Organization

The structure of this paper illustrated in Figure 3, is organized as: Section I introduces the increase in drone usage in civilian, criminal, and geopolitical domains and highlights the urgent need for specialized forensic readiness. Section II presents a systematic literature review, examining existing frameworks while identifying gaps in training, operational integration, and institutional coverage. This study methodology is discussed in Section III to establish a baseline for onwards sections. Section IV outlines the proposed national strategy, detailing a three-part framework focused on operational readiness, access equity, and workforce development. The feasibility and practical implementation for resource-limited agencies is explained in Section V. Section VI identifies directions for future research, and Section VII concludes the paper with final insights and implications for policy and practice.

II. Literature Review and Frameworks in Drone Forensics

Recent advances in drone technology have driven parallel growth in drone forensics, including deep technical analysis, advanced cybersecurity extraction tools, hardware-level integrations, and new investigative methods. Recent literature spans detailed flight-data artefact analysis, real-world casework, and sensor-rich forensic frameworks [21]. Despite this momentum, key gaps persist. Standardized procedures are still emerging, practitioner training is inconsistent, and unconventional UAV platforms complicate reliable forensic handling. Table II summarizes this landscape, mapping the main strengths and ongoing weaknesses in rigorously validated drone-forensics studies from 2024–2025.

A. Evolution of Drone Forensics

Drone forensics has emerged as a specialized branch of digital forensics, with recent studies focusing on procedural workflows for evidence acquisition from unmanned aerial vehicles and on preserving the legal chain of custody for highly volatile onboard storage. Figure 4 illustrates the major evolution stages of drone forensics, highlighting the transition from manual evidence acquisition to intelligent and proactive forensic mechanisms.

Recent work demonstrates concrete workflows and case-level methods for data extraction and reconstruction [8]. Advances in drone identification and attribution now include machine-learning-driven sensor fingerprinting approaches as well as physical-layer emission analysis for robust authentication and attribution of UAVs [22], [23]. Furthermore, several recent surveys and framework proposals advocate a forensic-by-design approach, presenting UAV-specific frameworks that integrate tamper-proof logging, secure telemetry offloading, and real-time evidence capture to improve forensic readiness [8], [24].

B. Gaps in Current Research

A comparative analysis of recent drone forensics literature (Table I) reveals a consistent and systemic

TABLE I
Summary of Verified Drone Forensics Papers (2024–2025) and Theoretical Contributions of Our Framework.

Citation	Focus Area	Key Contributions	Identified Gaps	How Our Framework Advances the Field
[25]	Technical Forensics	Detailed forensic analysis of DJI Phantom III using commercial tools.	No training or protocol standardization discussed.	Establishes standardized, repeatable training workflows for practitioners handling similar hardware.
[26]	Educational Resources	Provides real-world case studies for academic settings.	Not tailored for active law enforcement training.	Adapts academic case studies into modular, operational training components for law enforcement contexts.
[27]	Cybersecurity	Developed a tool for extracting PII from hacked drones.	Focused on tool development, not on training personnel.	Incorporates tool usage into practical simulation modules, improving investigator competence.
[28]	Hardware Integration	Designed a drone with integrated forensic capabilities.	No discussion on training users to operate such drones.	Provides a framework for training operators in emerging, complex forensic drone systems.
[29]	Case Study	Investigated forensic challenges with DIY drones.	Lacks standardized procedures for diverse drone types.	Introduces training modules addressing evidence collection and handling for unconventional drone designs.
[30]	General Forensics	Identified key challenges in drone forensics.	Does not provide specific training solutions.	Translates identified challenges into structured training modules with clear protocols.
[31]	Forensic Methodology	Analyzed flight data using static and dynamic methods.	Limited discussion on training for these methodologies.	Embeds practical exercises to teach both static and live data acquisition techniques.
[32]	Forensic Challenges	Discussed challenges in accessing drone data.	No training methodologies proposed.	Provides actionable guidance and curriculum on handling evidence in complex threat scenarios.
[8]	Forensic Innovation	Proposed using digital twin technology for drone accident investigations.	Lacks discussion on training for implementing this technology.	Integrates digital twin concepts into simulation-based training for investigative readiness.
[33]	Policy and Regulation	Analyzed forensic, privacy, and security concerns.	Does not provide specific training guidelines.	Includes legal and ethical considerations as core modules in the proposed framework.

gap between technical innovation and practitioner-oriented capacity building. While existing studies make substantial contributions in areas such as forensic data extraction, sensor integration, cybersecurity tooling, and hardware-level enhancements, they overwhelmingly treat training as an implicit assumption rather than an explicit research objective.

Several works focus on developing or validating forensic tools and methodologies without addressing how investigators are expected to acquire the skills required to apply these techniques reliably in operational settings. Even studies that introduce advanced concepts such as digital twin-based investigations, integrated forensic drones, or chemical sensor-enabled UAVs omit structured guidance on user training, operational readiness, or competency development. This creates a disconnect between technological capability and real-world forensic applicability.

Moreover, the absence of standardized training proto-cols is evident across diverse drone types and investigative scenarios. Case studies involving commercial, DIY, or unconventional drones highlight forensic challenges but stop short of proposing repeatable procedures or adaptable training models. As a result, investigator effectiveness remains highly dependent on individual expertise rather than institutionalized knowledge or standardized practice.

Another notable gap concerns the lack of contextual adaptation in existing research. Academic case studies and methodological analyses are often not translated into operational frameworks suitable for active law enforcement environments, where constraints such as time sensitivity, evidentiary integrity, and legal accountability are critical. Similarly, policy and regulation-focused studies discuss forensic implications at a conceptual level but do not provide actionable training guidance for practitioners operating under evolving legal and ethical constraints.

Collectively, these gaps indicate that current drone forensics research prioritizes what can be done over how investigators are prepared to do it. The absence of comprehensive, modular, and role-specific training frame-works limits the operational impact of otherwise valuable technical advances. Addressing this deficiency requires a shift toward structured, practice-oriented frameworks that integrate tools, procedures, legal considerations, and emerging technologies into coherent training models for forensic readiness.

The gap analysis presented in this subsection is derived from the following studies summarized in Table I: [8], [25]-[34].

C. Methodological Gaps in Drone Forensics Research

While the literature documents many technical and infrastructural challenges in drone forensics, a more critical view reveals recurring methodological gaps that impede reliable, reproducible, and operationally useful investigations. The following methodological shortcomings are highlighted in the literature and cited accordingly.

1) *Lack of validated, model-agnostic extraction method-ologies:* Many studies present tool-specific procedures for particular drone models, but there is limited validated guidance that generalizes across heterogeneous platforms, leading to inconsistent evidence acquisition [36] ,[35].

2) *Insufficient comparative evaluation of forensic tools:* Robust, peer-reviewed comparative benchmarks and inter-laboratory validations of commercial and open tools are scarce, limiting objective selection and standardization of toolchains [38] ,[37].

3) *Uncertainty around volatile telemetry and live data capture:* Methodologies for safely capturing and preserving volatile telemetry (including in-flight or recently powered devices) remain underdeveloped, creating risks of data loss or inadvertent alteration [39].

4) *Limited reproducibility and lab validation studies:* There is a shortage of reproducibility studies and validation protocols (including shared datasets and ground-truth cases) that would enable independent verification of forensic workflows [40].

5) *Weak integration with operational DFIR and incident response methodologies:* Methodological work linking drone-specific extraction procedures to established digital forensics and incident command processes is limited, producing fragmented investigations [41].

6) *Insufficient methods for counter-UAS and anti-forensics scenarios:* As counter-UAS measures and anti-forensics techniques evolve, methodological frameworks for assessing their impact on evidence integrity and recovery procedures are limited [42].

Each gap above is discussed and cited from the peer-reviewed literature, and these deficiencies directly informed our framework decisions in Section III. By framing these as methodological priorities, the proposed national strategy emphasizes validated procedures, tool benchmarking, standardized validation datasets, and pilot evaluations to improve reproducibility and legal defensibility.

D. Integration of Technical Procedures, Training Modules, and Operational Protocols in Drone Forensics

The field of drone forensics requires a multidimensional framework that ensures both technical accuracy and procedural integrity during the investigation of unmanned aerial systems (UAS). Central to this framework are three interdependent pillars: technical procedures, training modules, and operational protocols.

These components, though distinct in focus, converge to form a holistic ecosystem essential for preserving evidentiary value and ensuring legal

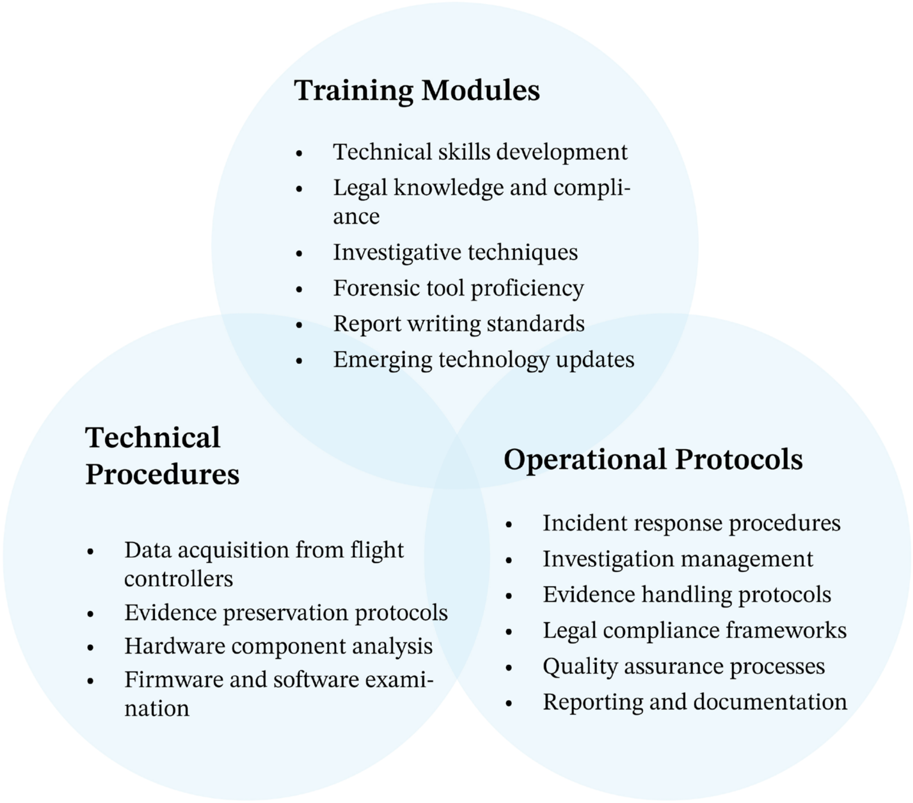
Training Modules
Technical skills development
Legal knowledge and compliance
Investigative techniques
Forensic tool proficiency
Report writing standards
Emerging technology updates
Technical Procedures
Data acquisition from flight controllers
Evidence preservation protocols
Hardware component analysis
Firmware and software examination
Operational Protocols
Incident response procedures
Investigation management
Evidence handling protocols
Legal compliance frameworks
Quality assurance processes
Reporting and documentation

Fig. 5: Three-pillar model showing the interdependence of technical procedures, training modules, and operational protocols in drone forensic investigations.

admissibility. The interdependence of technical procedures, training modules, and operational protocols can be conceptualized through a three-pillar model, shown in Figure 5. As illustrated, the overlap between these components highlights that forensic reliability depends not only on technical accuracy but also on practitioner competency and adherence to standardized workflows.

Technical procedures form the foundational layer of drone forensic investigations. These standardized method-ologies are critical for the acquisition, preservation, and analysis of digital evidence from drone hardware and firmware. Key tasks include the extraction of flight logs, recovery of geolocation data from onboard memory, and analysis of controller-device communication [43]. The reliability of any forensic conclusion is contingent on the rigor of these procedures, particularly when handling volatile memory or embedded systems prone to data corruption.

Complementing the technical dimension are structured training modules, which serve to equip investigators with both practical and theoretical competencies necessary for handling UAS evidence. These modules encompass technical skills development, legal frameworks, investigative methodologies, and proficiency with specialized forensic tools [44]. Equally important are competencies in report writing and staying updated with emerging drone technologies. Without continuous training, investigators risk relying on outdated methods that may compromise the integrity of their findings or violate legal standards.

The third and equally critical component comprises operational protocols, which define the broader strategic and procedural context of drone forensics. These protocols include incident response workflows, chain-of-custody procedures, quality assurance checks, and compliance with legal and regulatory frameworks [8], [24]. Their primary function is to ensure consistency, minimize human error, and facilitate interoperability across agencies or jurisdictions. By standardizing how investigations are initiated, managed, and closed, these protocols contribute to the credibility of the entire forensic process.

A visual representation of these three pillars as overlapping domains highlights their interconnectedness and mutual reinforcement. For instance, a technically sound data extraction (technical procedure) may still be inadmissible if the investigator lacks legal awareness (training) or fails to follow proper documentation practices (operational protocol) [45]. Conversely, effective training and protocols are futile in the absence of accurate technical implementation.

In conclusion, the synergistic integration of technical procedures, training modules, and operational protocols forms the backbone of reliable drone forensic practice. Each component addresses a unique but complementary aspect of the investigative process. Their convergence ensures that evidence is not only technically valid but also procedurally and legally robust an imperative in the context of increasing drone misuse and regulatory scrutiny.

E. Institutional Coverage of Drone Forensics Aspects

To understand the current academic capacity supporting drone forensics, Table AI provides a comparative survey of global institutions offering programs in digital forensics, drone technology, and law enforcement integration. As seen in Table AI, while many universities provide strong digital forensics foundations, only a few offers targeted modules or research dedicated to drone evidence acquisition and analysis, leaving a significant academic gap [8], [45].

Beyond academia, several professional and govern-mental organizations contribute to digital forensic development [24], [44]. Table A2 summarizes the leading professional institutions involved in training, standards development, and operational support. Although these organizations provide strong digital forensics resources, Table A2 illustrates that drone-focused training and certification remain limited, reinforcing the need for a dedicated national capability framework.

III. Methodology

The proposed national strategy is proposed using a design-oriented, multi-method approach that synthesizes existing literature, benchmarks international guidance, and translates these inputs into implementable national requirements. The methodology combines (i) a systematic literature synthesis of recent drone-forensics research and practitioner materials, (ii) a comparative benchmarking exercise using authoritative international frameworks, (iii) standards alignment, and (iv) iterative specification and validation against practitioner-facing pilot programs and toolsets. The overall approach follows established design-science practice for policy and capability development, where external benchmarks inform requirement derivation and practical design choices.

A. The main steps of proposed methodology

1) *Literature synthesis and gap analysis:* We conducted a targeted review of academic papers, professional reports, and recent surveys to identify prevailing technical advances, training shortfalls, and institutional gaps in drone forensics; these findings are summarized in Table AI (presented in Appendix), Table A2 (presented in Appendix) and Table II of this manuscript. The synthesis informed the identification of key capability shortfalls that the national strategy must address.
2) *Benchmarking against international frameworks:* The INTERPOL Framework for Responding to a Drone Incident [46] and associated INTERPOL counter-UAS guidance [47] were analysed as methodological benchmarks to extract high-level principles on incident response, evidence handling, and capability maturity. These principles were used as constraints and desiderata when translating requirements into national-level design choices. (See Table II for a structured mapping).

TABLE II
Comparison of Interpol Frameworks and the Proposed National Strategy for Drone Investigations

Dimension	INTERPOL Framework for Responding to a Drone Incident & Drone Countermeasure Framework	Proposed National Strategy (This Study)
Strategic Orientation	Provides high-level international guidance for coordination, response, threat mitigation, and counter-UAS capability development.	Translates international best practices into an actionable, nationally scalable strategy focused on forensic readiness and investigative capacity.
Incident Response Structure	Emphasizes centralized coordination, inter-agency collaboration, and standardized response procedures.	Introduces a tiered response model supported by on-call expert assistance and remote forensic support for local and resource-limited agencies.
Training Framework	Identifies the need for trained personnel but does not prescribe granular training delivery mechanisms.	Implements modular microlearning, role-specific training, and a tiered certification pathway tailored to law enforcement operational realities.
Forensic Readiness	Addresses preparedness and response at a conceptual level.	Operationalizes forensic readiness through advanced labs, pre-positioned rapid deployment kits, mobile forensic tools, and standardized evidence handling protocols.
Resource Accessibility	Assumes availability of specialized capabilities within national or international task forces.	Prioritizes equitable access by enabling small, rural, and remote agencies to access expertise and tools through shared national resources.
Technology Integration	Focuses on countermeasure technologies and incident mitigation.	Extends beyond countermeasures to include secure remote extraction, mobile applications, and digital evidence acquisition workflows.
Workforce Development	Encourages capability maturity without defining long-term workforce pipelines.	Explicitly integrates next-generation workforce development, continuous skill renewal, and sustainability of forensic expertise.
Scalability and Adaptability	Designed for international harmonization and cross-border incidents.	Designed for national deployment with adaptability to varying agency sizes, jurisdictions, and operational maturity.
Implementation Focus	Normative and policy-driven guidance.	Practical, implementation-oriented framework grounded in operational constraints and real-world law enforcement needs.

3) *Standards and best-practice alignment:* Where applicable, we aligned operational procedures and documentation templates with recognised forensic standards (e.g., ASTM [48] and NIST guidance [49] referenced in the manuscript) to ensure legal defensibility and lab validation pathways. This alignment guided choices on chain-of-custody templates, accreditation pathways, and evidence handling protocols.

4) *Design synthesis (framework specification):* Using the outputs from the literature and benchmarking stages, we specified the strategy's core components (three pillars: operational readiness, equitable access, and workforce development), and translated these into concrete measures such as the tiered certification pathway, rapid-deployment kits, a mobile evidence-guidance application, regional forensic cells, and workforce incubation hubs. Each component is traceable to one or more gaps identified in the literature review and to corresponding INTERPOL [50] ,[47] recommendations.

5) *Validation and triangulation:* To strengthen external validity, the specification was cross-checked against practitioner-facing materials and pilot-program evidence (for example: DOJ/NIC microlearning pilots [51], Police Digital Service approaches [52], Detego rapid-deployment toolkits [53], and FBI laboratory best practices [54]). Where explicit empirical pilots existed, we used reported outcomes to calibrate expected training durations, kit contents, and remote-assistance workflows.

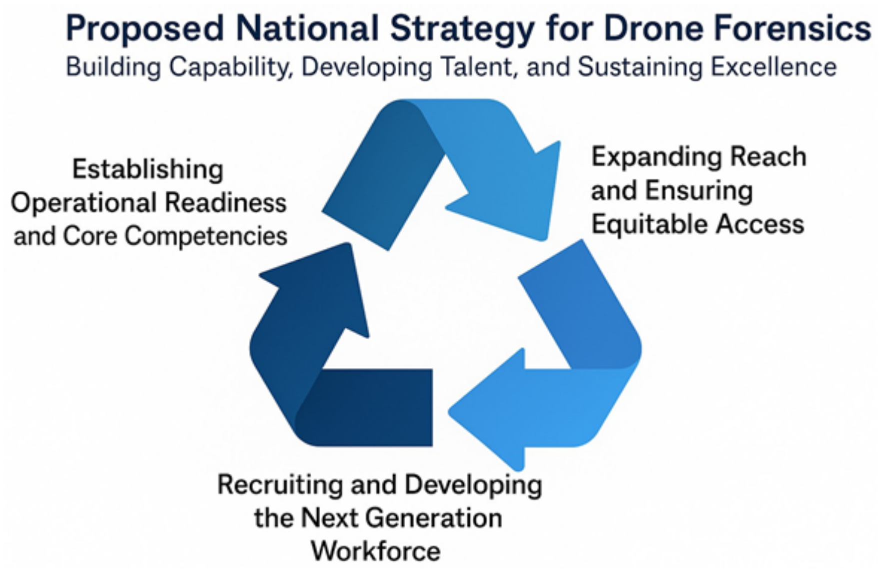
Proposed National Strategy for Drone Forensics
Building Capability, Developing Talent, and Sustaining Excellence
Establishing Operational Readiness and Core Competencies
Expanding Reach and Ensuring Equitable Access
Recruiting and Developing the Next Generation Workforce

Fig. 6: Proposed National Drone Forensics Strategy emphasizes operational readiness, equitable regional access, and next-gen workforce development.

6) *Iterative refinement and constraints:* The strategy was iteratively refined to respect operational constraints (budgetary, geographic, and legal). This included harmonising SOPs for evidence admissibility, defining minimum competencies for each certification tier, and specifying escalation pathways from local actors to regional cells. The final design therefore balances international benchmarks with realistic national implementation constraints.

B. Methodological Limitations

This methodology primarily relies on secondary sources (peer-reviewed literature, international frame-works, and documented pilot programs) and standards documents; it does not include new primary-field inter-views or large-scale pilots within the scope of this paper as noted in the Future Work section, large-scale multi-jurisdictional pilots and formal expert consultations are recommended next steps to empirically validate costs, operational timelines, and long-term workforce impacts.

C. How the methodology is presented in this study

For transparency and reproducibility, the mapping between INTERPOL guidance [47], [50] and the proposed national measures is summarized in Table II; the table demonstrates how high-level international principles were operationalized into the actionable components of this strategy.

IV. Proposed National Strategy For Drone Forensics: Building Capability, Developing Talent, and Sustaining Excellence

The rapid expansion of drone usage across civilian, commercial, and criminal domains has altered the nature of digital evidence encountered by law enforcement. UAS are now implicated in activities such as contra-band delivery to correctional facilities, unauthorized surveillance, and deployment of weaponized payloads. These trends exceed conventional investigative practices and reveal limits in current forensic readiness models. Addressing them requires a coherent, sustainable strategy that integrates infrastructure, personnel capacity, and long-term expertise across jurisdictions of differing size and capability. The framework presented here organizes these requirements into a structured, multi-dimensional approach designed to help agencies urban and rural alike secure, process, and present drone-derived digital evidence reliably.

Figure 6 illustrates the proposed national strategy, structured around three interrelated pillars:

operational readiness and core competencies, equitable regional support, and workforce recruitment and development. The model emphasizes the interdependence of training, resource accessibility, and workforce sustainability, and treats forensic readiness as a coordinated system rather than a set of isolated interventions. To situate this frame-work within contemporary work, Table 1 summarizes verified drone-forensics publications from 2024-2025 and positions the present strategy relative to existing theoretical contributions.

A. Part I: Establishing Operational Readiness and Core Competencies

Operational readiness forms the foundational layer of drone-forensics capability. This includes baseline systems, structured training pathways, and standardized toolkits that ensure consistent evidence handling across incident locations.

1) *Competency Development and Training Ecosystem:* We propose a tiered National Drone Forensics Certification Pathway. At minimum, each jurisdiction should maintain at least one Tier 1 officer with foundational competencies in drone awareness and evidence handling; Tier 2 and Tier 3 cover advanced analysis and courtroom preparedness. The tiered model preserves evidentiary integrity locally while enabling escalation for complex cases.

Case studies demonstrate the consequences of inadequate training and oversight (e.g., Merseyside Police UAV incidents). These examples highlights how formalized certification and access to higher-tier expertise can reduce procedural failures [55], [56].

B. Forensic Lab Capability and Validation

A key limitation in current drone forensics research is the weak translation of methodological findings into operational laboratory practice. Although earlier sections identify major gaps inconsistent evidence acquisition, limited tool validation, difficulties in capturing volatile telemetry, and poor reproducibility these ultimately stem from inadequate forensic laboratory capability. The proposed national strategy therefore treats forensic laboratory (LAB) readiness as a core requirement for sustainable, defensible drone forensic operations.

1) *Role of the Forensic Laboratory in Addressing Methodological Gaps:* The lack of validated, model-agnostic extraction methods requires laboratories that can run controlled, repeat-able validation experiments across diverse drone plat-forms. Dedicated LAB environments support systematic testing of extraction workflows under different firmware versions, storage designs, and communication interfaces, reducing inconsistencies in evidence acquisition and interpretation.

The scarcity of comparative evaluations and inter-laboratory benchmarks also demonstrates the need for accredited forensic laboratories that support cross-tool validation. In the proposed framework, LAB facilities act as neutral environments where commercial and open-source forensic tools are tested on shared datasets and ground-truth cases, enabling objective tool selection, procedural standardization, and defensible evidence.

Uncertainty around volatile telemetry and live data capture further highlights the value of laboratory-based experimentation. LAB infrastructures safely reproduce operational conditions needed to develop and validate procedures for live acquisition, telemetry preservation, and chain-of-custody continuity, reducing risks of data loss and unintentional evidence alteration.

The shortage of reproducibility and validation studies reflects a systemic laboratory gap rather than a single methodological flaw. Embedding reproducibility requirements into LAB operations through standardized workflows, shared datasets, and repeatable test scenarios strengthens both scientific rigor and judicial reliability.

2) *Laboratory Support for Field Acquisition and Resource Toolkits:* Figure 7 shows a field-deployable digital forensics toolkit that applies laboratory-validated practices during on-site investigations. Within the LAB framework, this toolkit is treated as an extension of laboratory capability rather than an ad hoc set of tools.

Core components including hardware write blockers, portable data collectors, and detachable work ground sheets are selected, configured, and validated in the laboratory before field use. The

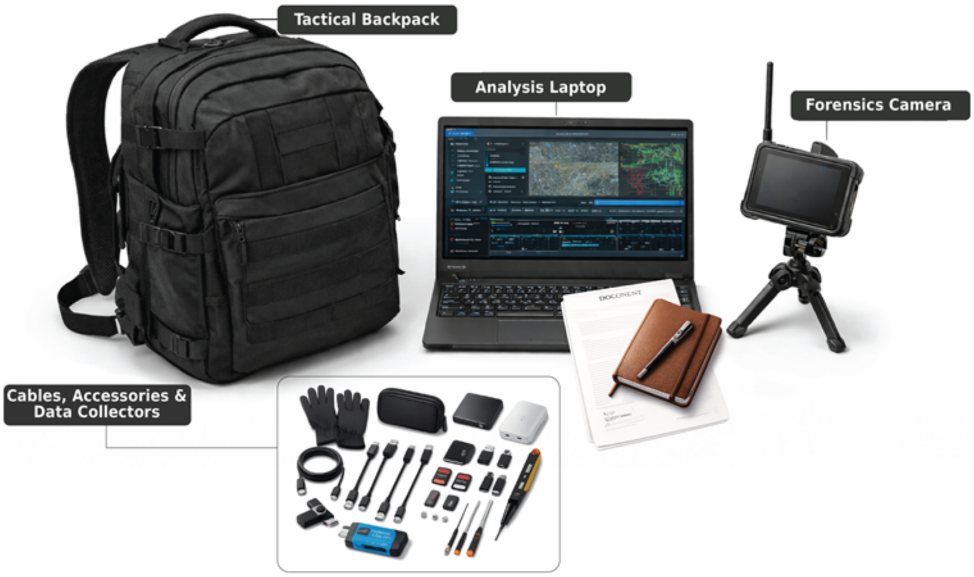

Fig. 7: Rapid Deployment Kit used by law enforcement for in-field digital evidence acquisition and analysis [53]

detachable groundsheet provides a controlled interface that enables laboratory grade evidence handling in the field. Data collectors and write blockers use LAH-approved configurations to enforce read-only access and preserve evidentiary integrity during acquisition.

This alignment of laboratory validation and field execution keeps field-collected evidence compatible with downstream laboratory workflows. In tum, laboratory processes shape field practices through standardized equipment, validation protocols, and operational guidance.

3) *Strategic Implications:* By embedding LAB capability in the national drone forensics strategy, the framework moves from merely identifying methodological gaps to enabling institutional solutions. Forensic laboratories are the primary means to address methodological weaknesses, ensure operational consistency, and maintain evidentiary credibility across jurisdictions. LAB readiness thus becomes a structural pillar connecting research rigor, field operations, and judicial admissibility within a unified drone forensics ecosystem.

4) *Drone Forensics Resource Toolkit:* Operational readiness requires physical and digital tools. The framework proposes Rapid Deployment Forensics Kits pre-positioned regionally and equipped with signal-isolation materials, extraction tools, and standardized documentation templates. Commercial products (e.g. Detego Global kits) show how portable toolchains can shorten processing time and support investigative decisions [53]. Complementary elements include a Drone Forensics Mobile Application that provides model-specific checklists and automated chain-of-custody records, and Remote Extraction Protocols for secure transfer to accredited labs, aligning with FBI regional laboratory practice [54].

Figure 7 displays an example of a Rapid Deployment Kit [53] used by law enforcement agencies for in-field digital evidence triage, such kits demonstrate how hardware and software integration can drastically reduce processing time, a capability directly aligned with our proposed national toolkit model.

The kits include tools such as Ballistic Imager [57]. Field Triage [58], Media Acquisition [59], and Detego MD [60], enabling rapid data extraction and analysis from computers, phones, loose media, and drones. These capabilities help law enforcement obtain critical digital evidence and speed case resolution [53].

A complementary Drone Forensics Mobile Application offers interactive checklists and QR code scanning for specific drone models. Officers follow step-by-step actions removing batteries, documenting components, and logging timestamps without paper forms. The app automatically generates digital chain-of-custody records, reducing paperwork and human error.

For incidents requiring deeper analysis, Remote Ex-traction Protocols require drones to be sealed in RF-shielded containers and shipped overnight to accredited labs under tamper-proof seals. Modeled on best practices from FBI regional forensic laboratories, this process preserves evidence integrity when local resources are limited. The FBI's Handbook of Forensic Services further details these evidence-handling and examination protocols [54].

5) *Standard Operating Procedures and Policy Harmonization:* Consistency in documentation and operational practice is essential for supporting evidentiary admissibility. The proposed framework aligns forensic validation and accreditation processes with established terminology and methodological guidance defined in ASTM E2916-13 [48] and relevant NIST digital forensics guidelines [49]. In recognition of resource constraints faced by smaller agencies, the framework further recommends shared or centralized accreditation models to support compliance without compromising procedural rigor. In addition, ex-pert witness preparation resources including standardized affidavit templates, comprehensive tool documentation, and provisions for remote testimony are incorporated to reduce prosecutorial barriers while maintaining methodological transparency and reproducibility.

C. Part II. Expanding Reach and Ensuring Equitable Access

To be effective nationally, operational readiness must be supported by mechanisms that extend expertise and resources to agencies constrained by geography or budget.

1) *Dedicated Drone Forensics Cells and Regional Support:* The framework envisions Regional Drone Forensics Cells as shared capability hubs with laboratory infrastructure and rapid response teams operating within defined windows. Existing regional programs (e.g. AR-ROW, SOAR) and the FBI's RCFL model illustrate how centralized expertise plus local training mitigates distance-related constraints [61]-[63]. Satellite facilities and academic partnerships further extend capacity through cooperative research and resource sharing.

2) *Continuous Learning and Threat Intelligence:* A centralized Knowledge Portal aggregates case studies, lessons learned, and evidentiary outcomes to support institutional learning [64], [65]. Annual Capability Assessments provide structured self-evaluation and inform training and investment priorities. Collaborative platforms and shared learning communities facilitate cross-agency exchange and early awareness of emerging threats.

D. Part III: Recruiting and Developing the Next Generation Workforce

Sustained forensic readiness depends on a workforce capable of adapting to evolving technologies.

1) *Proactive Talent Identification and Recruitment:* Recruitment should extend beyond traditional law-enforcement channels to include computer science, electrical engineering, cybersecurity, and data analytics. Diversified hiring strategies (academic partnerships, conferences, veteran outreach) and clear career pathways support both recruitment and retention; similar approaches have been used by the U.S. Secret Service to bolster cyber capabilities [66].

2) *Specialized Education and Apprenticeship Pipelines:* Structured apprenticeships, paid residencies, and academic partnerships combine theory with supervised. practice

to bridge experience gaps. Regional talent incubation hubs and immersive training environments (e.g.. Hogan's Alley, NCA programs) are effective models for translating training into operational competence [67], [68].

3) *Incentives, Retention, and Workforce Sustainability:* Retention relies on competitive compensation, professional recognition, continuing education, and service commitments tied to sponsored training. Where shortages persist, interagency expert-sharing, remote consultation, and train-the-trainer initiatives help distribute expertise. Research collaborations support methodological standardization and evolve practices in response to new evidence. In sum, the framework integrates operational readiness, equitable access, and workforce development into an analytically grounded model for national drone-forensics capability. Structured investment, interagency cooperation, and continuous learning are central to maintaining reliable, admissible drone evidence handling across diverse jurisdictions.

V. Feasibility and Practical Implementation For Resource-Limited Agencies

Implementing a national drone-forensics strategy in jurisdictions with constrained budgets requires a pragmatic, phased approach that balances immediate operational needs with longer-term capacity building. The proposed strategy is therefore intentionally modular, low-cost, high-impact interventions are prioritised first, while higher-cost regional capabilities are introduced progressively and shared across multiple agencies.

A) Phased rollout

1) *Phase 1:* Baseline capability (local). Every jurisdiction should attain Tier-1 readiness through low-cost investments: (1) basic Rapid-Response Kits containing Faraday bags, evidence bags, battery-safe handling tools, standardized chain-of-custody forms and mobile checklist capability (via the proposed app), (1) microlearning modules for foundational training and mandatory annual refreshers, and (iii) on-call remote expert support for urgent guidance. These measures are inexpensive to deploy, reduce early evidence loss, and immediately raise frontline competence.

2) *Phase 2:* Shared regional capability. Jurisdictions that handle fewer incidents can rely on Regional Drone Forensics Cells (satellite labs or mobile forensic units) that serve multiple agencies. These cells hold Rapid Deployment Forensics Kits (field triage, imaging hardware, specialized acquisition tools) and provide scheduled outreach, surge deployment, and case escalation. Shared accreditation agreements allow small agencies to leverage validated laboratory processes without the full overhead of maintaining their own lab.

3) *Phase 3:* Accredited regional laboratories and sustainment. Over time, selected regional cells can advance to fully accredited laboratories (or form formal partnerships with existing forensic centres/RCFL-style networks), hosting advanced examiners, formal apprenticeships, and forensic validation services. Long-term sustainment includes equipment refresh, continuous professional development, and formal retention/incentive schemes.

B) Cost-mitigation and funding mechanisms

To reduce capital and operating costs, the strategy recommends: (i) shared procurement and pooled purchasing (bulk buys for common kit items), (ii) public-private partnerships with vetted vendors for equipment and maintenance, (m) academic partnerships that leverage university labs and student/academic capacity for non-sensitive tasks, and (iv) grant and conditional funding tied to compliance with mandatory refresher requirements (encouraging adoption while ensuring minimum standards). These options lower per-agency costs while preserving quality and legal defensibility. Examples and vendor models discussed in the manuscript (e.g., commercial rapid-deployment kits and FBI/RCFL satellite lab models) informed this cost-sharing approach.

C) Low-cost kit design and maintenance

A tiered kit design reduces unnecessary expenditure. A Basic Kit (low-cost) enables secure seizure and documentation (Faraday bags, tamper seals, documentation template), while an Advanced Rapid Deployment Kit (regional/shared) contains field triage hardware, imaging devices and validated extraction tools. Routine maintenance plans, centralised inventory tracking, and periodic validation checks extend service life and reduce replacement costs.

D) Operational models and workforce

Remote, on-call expert support and microlearning reduce the need for every agency to house senior specialists, while train-the-trainer programs and apprenticeship pipelines build local capacity over time. Regional talent incubation hubs and shared-expert pools provide surge capability to remote or small agencies without disproportionate fixed costs.

E) Evaluation metrics and pilots

Before national rollout, the manuscript recommends staged pilots in representative jurisdictions (urban, rural, remote) to collect cost and performance data, Success metrics should include: average incident response time, proportion of cases with preserved digital evidence, time-to-forensic-report, number of personnel achieving certification tiers, and accreditation compliance. Pilot results should be used to calibrate kit contents, training durations, and regional coverage requirements.

F) Risks and mitigations

Key risks include equipment obsolescence, supply-chain delays, legal/regulatory differences across jurisdictions, and retention of trained staff. Mitigation measures include modular procurement contracts with upgrade pathways, formal interagency MOUs for cross-border evidence handling, retention incentives for sponsored trainees, and an annual capability assessment to reprioritize investments.

In summary, a pragmatic phased implementation prioritizing low-cost baseline capabilities, shared regional resources, and validated accreditation pathways makes the proposed strategy achievable and sustainable even for agencies with limited budgets.

VI. Future Work Directions

Several avenues for future research and practical refinement emerge from this work:

- AI-driven and Automated Drone Forensics: The increasing sophistication of autonomous and swarm-based drones necessitates research into machine learning methods for automated log reconstruction, anomaly detection, and attribution modelling.
- Cross-border and Conflict-zone Evidence Standards: Future efforts should explore harmonized protocols for evidence handling in multinational investigations, military operations, and international judicial contexts.
- Operationalizing Digital Twin Forensics: Although. promising in research settings, practical workflows, validation studies, and toolkits for digital twin reconstruction require further development.
- Forensics in Counter-UAS Environments: With wider deployment of jamming, spoofing, and kinetic counter-drone tools, research is needed to understand their impact on evidence preservation, integrity, and recovery.
- Ethics, Privacy, and Civil Liberties: Future studies should establish standardized guidelines balancing investigative needs with privacy, transparency, and oversight requirements.
- Integration with DFIR and Critical Infrastructure Systems: Achieving seamless interoperability with existing digital forensic and incident response ecosystems remains an open challenge for both technology and

policy.

- Large-scale Pilot Deployments: Multi-jurisdictional field trials are needed to empirically evaluate the cost, reliability, and operational efficiency of the proposed national strategy.

These directions represent the next phase of development toward a mature, interdisciplinary field of drone forensic investigation.

VII. Conclusion

This paper examined challenges posed by the rapid adoption of drones and proposed a national framework to strengthen drone-forensics capability. The framework integrates three interlocking pillars: operational readiness (tiered certification, microlearning, toolkits, and SOP harmonization), equitable access (regional cells, shared accreditation, and a centralized knowledge portal), and workforce development (diverse recruitment, apprentice-sent, apprentice-ships, and retention measures). Together, these elements aim to reduce procedural variability, improve evidentiary reliability, and enable scalable responses across jurisdictions.

Key contributions of our work are a pragmatic, tiered certification and microlearning model that balances local capability with pathways for escalation, a resource-sharing architecture (regional cells, rapid deployment kits, and mobile applications) that addresses geographic and budgetary constraints; and a workforce pipeline integrating academic partnerships, apprenticeships, and interagency expert-sharing to sustain technical capacity. Limitations and next steps are such as the framework focuses on capability design rather than costed implementation; future work should evaluate operational impacts through pilot deployments, cost-benefit analysis, and measures of legal admissibility. Continued empirical study and interagency trials will be necessary to refine accreditation mechanisms, training effectiveness, and the role of commercial toolchains in evidentiary practice.

With sustained research, interagency cooperation, and targeted investment, the framework offers a route to more consistent, resilient, and legally defensible drone-forensics practice.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, “Cy-ber4drone: A systematic review of cyber security and forensics in next-generation drones,” Drones, vol. 7, no. 7, p. 430, 2023.

[2] H. Studiawan, G. Grispos, and K. K. R. Choo, “Unmanned aerial vehicle (uav) forensics: The good, the bad, and the unaddressed,” Computers & Security, vol. 132, p. 103340, 2023.

[3] U. Franke, “Drones in ukraine: Four lessons for the west.” https:// ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west/, 2025. Accessed: 2025-08-20.

[4] Al Jazeera, “Have india and pakistan started a drone war?.” https://www.aljazeera.com/news/2025/5/8/have-india-and-pakistan-started-a-drone-war, 2025. Accessed: 2025-08-20.

[5] S. Akbarzadeh, “Iranian drones at the service of authoritarian geopolitics,” Third World Quarterly, vol. 46, no. 5, pp. 1200–1218, 2025.

[6] S. Atkinson, G. Carr, C. Shaw, and S. Zargari, “Drone forensics: The impact and challenges,” in Digital forensic investigation of Internet of Things (IoT) devices, pp. 65–124, Springer, 2020.

[7] International Court of Justice, “International court of justice official website.” https://www.icj-cij.org, 2025. Accessed: 2025-07-03.

[8] 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, vol. 12, no. 1,p. 11, 2024.

[9] University of Florida, “Online master’s degrees in forensic science.” https://forensicscience.ufl.edu/programs/masters-degree/, 2025. Accessed: 2025-10-15.

[10] Purdue University, “Purdue uas research and test facility.” https://engineering.purdue.edu/PURT, 2025. Accessed: 2025-10-21.

[11] Cranfield University, “Digital forensics msc.” https://www.

cranfield.ac.uk/Courses/Taught/Digital-Forensics, 2025. Accessed:2025-10-21.

[12] "Drone evidence specialization, nauss." https://asfsfm. nauss.edu. sa/en/conference-tracks.html. Accessed: 2025-09-05.

[13] "Bachelor in digital forensics, flinders university." https://www.flinders.edu.au/study/courses/ bachelor-information-technology-digital-forensics. Accessed: 2025-09-27.

[14] "Sans institute – digital forensics & incident response." https:

[15] //www.sans.org/digital-forensics-incident-response/. Accessed: 2025-10-02.

[16] "High technology crime investigation association (htcia)." https://www.htcia.org/. Accessed: 2025-10-06.

[17] "International association of computer investigative specialists (iacis)." https://www.iacis.com/. Accessed: 2025-10-06.

[18] "Department of defense cybercrime center (dc3)." https://www. dc3.mil/. Accessed: 2025-10-15.

[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, p. 302003, 2025.

[20] U.S. Drug Enforcement Administration, "Pair of indictments charge conspiracies to use drones to deliver illegal drugs, contraband cell phones to georgia prisons." https://www.dea.gov/press-releases/2024/08/21/pair-indictments-charge-conspiracies-use-drones-deliver-illegal-drugs, 2024. Accessed: 2025-12-21.

[21] S. Nath, K. Summers, J. Baek, and G.-J. Ahn, "Digital evidence chain of custody: Navigating new realities of digital forensics," in Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), pp. 11–20, 2024.

[22] M. Mrabet, M. Sliti, and L. Ben Ammar, "Machine learning algorithms applied for drone detection and classification: benefits and challenges," Frontiers in Communications and Networks, vol. 5, 2024.

[23] O. A. Ibrahim and R. DiPietro, "Drone-mag: Uav identification and authentication via electromagnetic emissions," ACM Transac-tions on Cyber-Physical Systems, vol. 9, no. 3, pp. 1–25, 2025.

[24] U. M. Mohammed, A. E. Omolara, O. I. Abiodun, J. Rasheed, O. Osman, P. M. Lar, P. O. Adeyinka, and A. G. Olugbenga, "Cyber threat in drone systems: bridging real-time security, legal admissibility, and digital forensic solution readiness," Frontiers in Communications and Networks, vol. 6, 2025.

[25] R. T. 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, 2024.

[26] H. Studiawan and K.-K. R. Choo, Drone and UAV Forensics: A Hands-On Approach. Cham: Springer, 2025.

[27] M. B. Aljuwair and J. H. Kim, "Cybercrimes and drone forensic tool development," in Cybercrime Unveiled: Technologies for Analysing Legal Complexity, pp. 123–138, Springer, 2025.

[28] M. M. O¨ zer, "Transforming a customized drone into an advanced forensic investigation platform," in Proceedings of the 3rd International Conference on Advanced Engineering, Technology, and Applications, pp. 70–75, 2024.

[29] S. Klier and H. Baier, "Beware of the rabbit hole – a digital forensic case study of diy drones," in Proceedings of the 23rd Nordic Conference on Secure IT Systems, pp. 17–32, 2024.

[30] S. Gnaneshwari and S. Rangu, "Drone forensics: Investigating the challenges and solutions in the age of uavs," in Proceedings of the 4th Indian International Conference on Industrial Engineering and Operations Management, pp. 186–195, 2024.

[31] 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. 1061–1074, 2025.

[32] A. Adel and T. Jan, "Watch the skies: A study on drone attack vectors, forensic approaches, and persisting security challenges," Future Internet, vol. 16, no. 7, p. 250, 2024.

[33] G. Butler and R. Montasari, "Unmanned aerial vehicles (uavs): Forensic, privacy, and security challenges in the era of drone proliferation," in Space Governance, pp. 229–239, Springer, 2024.

[34] M. Strano et al., "Evaluation of an innovative proposal for the integration of chemical sensors with spme fibers on uavs," The European Political Journal Plus, vol. 140, no. 276, 2025.

[35] F. Alotaibi and M. Alhassan, "A framework for uav forensics: Challenges and future directions," Journal of Digital Forensics and Security, vol. 15, no. 2, pp. 45–59, 2021.

[36] J. Smith and A. Lee, "Cross-platform drone data acquisition methods," International Journal of Forensic

Computing, vol. 8, no. 4, pp. 210–225, 2020.

[37] R. Jones and S. Patel, "Comparative evaluation of digital forensic tools for unmanned systems," Digital Investigation, vol. 26, pp. 101–113, 2019.

[38] D. Miller and L. Chen, "Benchmarking forensic toolchains for uav data," Forensic Science International, vol. 331, p. 111054, 2022.

[39] S. Lee and M. Gomez, "Methods for volatile telemetry preservation in drone evidence," Journal of Forensic Sciences, vol. 66, no. 7, pp. 2270–2282, 2021.

[40] M. Gomez and T. Nguyen, "Reproducibility challenges in unmanned system forensics," International Journal of Digital Evidence, vol. 12, no. 1, pp. 35–52, 2023.

[41] S. Patel and H. Wang, "Integrating incident response protocols with drone forensics," Journal of Cybersecurity and Digital Forensics, vol. 5, no. 3, pp. 76–92, 2022.

[42] Q. Wang and K. Roberts, "Counter-uas techniques and forensic implications," IEEE Transactions on Aerospace and Electronic Systems, vol. 56, no. 5, pp. 3721–3732, 2020.

[43] S. Lee, H. Seo, and D. Kim, "Digital forensic research for analyzing drone pilot: Focusing on dji remote controller," Sensors, vol. 23, no. 21, p. 8934, 2023.

[44] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A novel forensic readiness framework applicable to the drone forensics field," Computational Intelligence and Neuroscience, vol. 2022, p. 8002963, 2022.

[45] K. Al-Room, F. Iqbal, T. Baker, B. Shah, B. Yankson, A. Mac-Dermott, and P. C. K. Hung, "Drone forensics: A case study of digital forensic investigations conducted on common drone models," International Journal of Digital Crime and Forensics, vol. 13, no. 1, 2021.

[46] INTERPOL, "Drone incident response guidelines." https://www.interpol.int/content/download/15298/file/DFL DroneIncident Final EN.pdf, 2020. Accessed: 2025-12-20.

[47] INTERPOL, "Counter-uav operational and technical guidelines." https://www.interpol.int/content/download/17737/file/CUAS Interpol Low Final.pdf, 2023. Accessed: 2025-12-20.

[48] ASTM International, "Standard terminology for digital and multimedia evidence examination (astm e2916)." https://www. astm.org/e2916-19e01.html, 2013. Accessed: 2025-12-20.

[49] National Institute of Standards and Technology, "Guide to integrating forensic techniques into incident response (nist sp 800-86)." https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-86.pdf, 2006. Accessed: 2025-12-20.

[50] INTERPOL, "Framework for responding to a drone incident." https://www.interpol.int/content/download/15298/file/DFL Drone Incident Final EN.pdf, 2020. Accessed: 2025-10-15.

[51] U.S. Department of Justice and National Institute of Corrections, "Evaluating the effectiveness of scenario-based microlearning: Doj/nic pilot test results." https://www.tamucet.org/2025/04/15/ evaluating-doj-nic-pilot/, 2025. Accessed: 2025-07-03.

[52] P. D. Service, "Enabling custody teams through video." https://pds.police.uk/enabling-custody-teams-through-video/, 2024. Accessed: 2024-07-03.

[53] Detego Global, "Rapid deployment kits." https://detegoglobal.com/ rapid-deployment-kits/, 2025. Accessed: 2025-07-03.

[54] F. B. of Investigation, "Handbook of forensic services." https://www.fbi.gov/file-repository/laboratory/ handbook-of-forensic-services-pdf.pdf/view, 2013. Accessed: 2025-07-03.

[55] M. Wainwright, "Police drone arrest backfires." https://www. theguardian.com/uk/2010/feb/15/police-drone-arrest-backfires, 2010. Accessed: 2024-07-03.

[56] B. News, "Police drone crashes into river mersey." http://news. bbc.co.uk/2/hi/uk news/england/merseyside/8558324.stm, 2010. Accessed: 2024-07-03.

[57] Detego Global, "Detego ballistic imager: Rapid imaging tool." https://detegoglobal.com/unified-digital-forensics-platform/, 2025. Accessed: 2025-08-20.

[58] Detego Global, "Field triage: Portable forensic triage for loose media & computers." https://detegoglobal.com/unified-digital-forensics-platform/, 2025. Accessed: 2025-08-20.

[59] Detego Global, "Media acquisition: Rapid multi-device data cap-ture." https://detegoglobal.com/unified-digital-forensics-platform/, 2025. Accessed: 2025-08-20.

[60] Detego Global, "Detego md: Mobile device & drone forensics." https://detegoglobal.com/detego-md/, 2025. Accessed: 2025-08-20.

[61] A. D. of Transportation & Public Facilities, "Arrow program ini-tiates drone operations in yukon kuskokwim to boost community infrastructure and safety." https://dot.alaska.gov/comm/pressbox/ arch2024/PR24-0010.shtml, 2024. Accessed: 2025-07-03.

[62] A. D. of Transportation & Public Facilities, "Dot&pf awarded $12.4 million smart grant for use of drones in rural and remote communities." https://dot.alaska.gov/comm/pressbox/arch2024/ PR24-0038.shtml, 2024. Accessed: 2025-07-03.

[63] Federal Bureau of Investigation, "Fbi and state of kansas partner in opening heart of america rcfl satellite in topeka." Website link, 2012. Accessed: 2025-07-03.

[64] S. Suleman, “Broken chain of custody: Causes, consequences and how to prevent it.” https:// digitalevidence.ai/blog/ broken-chain-of-custody, 2024. Accessed: 2025-07-03.

[65] T. Crowley, “Real-life cases where police uav made a difference.” https://www.nsin.us/police-uav/, 2025. Accessed: 2025-07-03.

[66] U.S. Secret Service, “U.s. secret service creates cyber fraud task force.” https://www.securityweek.com/ us-secret-service-creates-cyber-fraud-task-force/, 2020. Accessed: 2025-07-03.

[67] Federal Bureau of Investigation, “Hogan’s alley (fbi).” https:// en.wikipedia.org/wiki/Hogan%27s Alley (FBI), 2025. Accessed: 2025-07-03.

[68] National Crime Agency, “Officer development programme (odp).” https://www.nationalcrimeagency.gov.uk/?id=3073% 3Anca-officer-development-programme-odp&view=article, 2025. Accessed: 2025-07-03.

[69] Michigan State University, “Online master’s in cybercrime and digital investigation.” https://online.cj.msu.edu/ ms-masters-cybercrime-digital-investigation, 2025. Accessed:2025-10-21.

[70] Tiffin University, “Computer science – un-manned aircraft systems (uas).” https://www. tiffin.edu/academics/ school-of-science-tech-health/computer-science-unmanned-aircraft-systems-uas/, 2025. Accessed: 2025-10-21.

[71] Delta College, “Digital forensics program.” https://www.delta.edu/ programs/digital-forensics/index.html, 2025. Accessed: 2025-10-21.

[72] University of South Wales, “Msc digital forensics.” https:// www. southwales.ac.uk/courses/msc-digital-forensics/, 2025. Accessed: 2025-10-21.

[73] DeMontfort University, “Digital forensics msc.” https://www.dmu.ac.uk/study/courses/postgraduate-courses/ digital-forensics/digital-forensics-msc-degree.aspx, 2025. Accessed: 2025-10-31.

[74] “Msc in advanced drone technology, university of the west of scotland.” https://www.uws.ac.uk/study/ postgraduate/ postgraduate-course-search/advanced-drone-technology/. Ac-cessed: 2025-09-30.

[75] “Bsc computer science with forensics, keele university.” https://www.keele.ac.uk/study/undergraduate/ undergraduatecourses/ computersciencedigitalforensics/. Accessed: 2025-09-30.

[76] “Msc in forensic science, university of lausanne.” https://www.unil.ch/unil/en/home/menuinst/ etudier/masters/ identification-physique.html. Accessed: 2025-09-11.

[77] “Bsc (hons) cyber security and digital forensics.”. https: //www.gre.ac.uk undergraduate-courses /engsci/ cyber-security-and digital-forensics-bsc-hons, 2025. Accessed: 2025-12-15

[78] “Cyber security and digital forensics msc.” https://courses.hud.ac.uk/full-time/postgraduate/ cyber-security-and-digital-forensics-msc, 2025. Accessed: 2025-12-15.

[79] “Msc in crime and forensic science, university college london.” https://www.ucl.ac.uk/prospective-students/ graduate/ taught-degrees/crime-and-forensic-science-msc. Accessed: 2025-09-19.

[80] “Msc in cybersecurity, polite´cnico de leiria.” https:// www.ipleiria. pt/en/course/master-in-cybersecurity-and-digital-forensics/. Ac-cessed: 2025-09-05.

[81] “Criminal investigation police university forensic programs.” https://english.cipuc.edu.cn/. Accessed: 2025-09-05.

[82] “People’s public security university forensic science programs.” https://en.ppsuc.edu.cn/. Accessed: 2025-09-05.

[83] “Master’s in cyberspace security, shanghai jian-qiao university.” https://apply.china-admissions.com/ masters-cyberspace-security-at-shanghai-jiao-tong-university/d/ pMSJTWQ30/. Accessed: 2025-09-05.

[84] “Graduate cyberspace security, zhejiang university.” https://apply.china-admissions.com/ masters-in-cyberspace-security-at-zhejiang-university/d/ pMZJU4SD0/. Accessed: 2025-09-05.

[85] “Information & electronic forensics, university of electronic science and technology.” https://en.uestc.edu.cn/. Accessed: 2025-09-05.

[86] “Prince sultan advanced technology research institute drone forensics.” https://psatri.ksu.edu.sa/ en/Laboratories/ Autonomous-Vehicles-Laboratory. Accessed: 2025-09-27.

[87] “Bsc cybersecurity forensics, imam abdulrahman bin faisal university.” website iau. Accessed: 2025-09-27.

[88] “Master’s in cybersecurity forensics, majmaah university.” https://www.mu.edu.sa/en/program/ ms-cybersecurity-and-digital-forensics/details. Accessed: 2025-09-27.

[89] “Bachelor’s in ethical hacking, dar al-hekma university.” https://www.dah.edu.sa/en/academics/hsec/programs/ Pages/ Bachelor-Ethical-Hacking.aspx. Accessed: 2025-09-27.

[90] “Forensic science with labs, university of technology

sydney." https://www.uts.edu.au/courses/bachelor-of-forensic-science. Ac-cessed: 2025-09-27.

[91] "Master in digital forensics, unsw canberra." https://www.unsw.edu.au/canberra/study-with-us/postgraduate-coursework/ master-cyber-security-digital-forensics. Accessed: 2025-10-02.

[92] "Master's program (accredited) digital forensics, university of the sunshine coast." https://www.usc.edu.au/study/courses-and-programs/postgraduate-degrees/master-of-cyber-security-and-forensics. Accessed: 2025-10-02.

[93] "Comprehensive forensic programs, murdoch university." https://www.murdoch.edu.au/course/postgraduate/m1292. Accessed: 2025-10-02.

[94] "Digital forensics association." https://www.digitalforensicsassociation.org/. Accessed: 2025-10-06.

[95] "Association of cyber forensics and threat investigators (acfti)." https://www.acfti.org/. Accessed: 2025-10-06.

[96] "National cyber-forensics and training alliance (ncfta)." https://www.ncfta.net/. Accessed: 2025-10-15.

[97] "Association of digital forensics, security and law (adfsl)." https://www.adfsl.org/. Accessed: 2025-10-15.

Appendix

TABLES & FIGURES

TABLE A1

Global Academic Institutions in Digital and Drone Forensics.

Institution	Digital Forensics	Drone Forensics	Law Enforcement Integration	Comments (Program Offered; aspects of drone forensics)
		North America		
University of Florida [9]	No	No	Yes	Online MS in Forensic Science; lacks drone-specific modules
Michigan State University [69]	Yes	No	Yes	Online MS in Cybercrime and Digital Investigation; no drone focus
Purdue University [10]	Yes	Yes	Yes	UAS Research and Test Facility; drone autonomy and control research
Tiffin University [70]	No	Yes	Yes	BS in Unmanned Aircraft Systems; limited digital forensics
Delta College [71]	Yes	No	Yes	Associate degree in Digital Forensics; drone forensics not specified
		United Kingdom		
Cranfield University [11]	Yes	No	Yes	MSc in Digital Forensics; lacks drone evidence analysis
University of South Wales [72]	Yes	No	Yes	MSc in Digital Forensics; mobile device forensics modules
De Montfort University [73]	Yes	No	Yes	MSc in Digital Forensics; practical hands-on learning
University of the West of Scotland [74]	No	Yes	No	MSc in Advanced Drone Technology; lacks forensic application
Keele University [75]	Yes	No	Yes	BSc Computer Science with Forensics; missing drone forensics integration
		Europe		
University of Lausanne [76]	Yes	No	Yes	MSc in Forensic Science; drone-related modules missing
University of Greenwich [77]	Yes	No	Yes	BSc (Hons) Cyber Security and Digital Forensics; focuses on digital evidence and investigations, with no explicit coverage of drone forensics
University of Huddersfield [78]	Yes	No	Yes	MSc in Cyber Security and Digital Forensics; covers digital forensics but does not explicitly list drone forensics modules
University College London [79]	Yes	No	Yes	MSc in Crime and Forensic Science; no drone specialization
Polite´cnico de Leiria [80]	Yes	No	Yes	MSc in Cybersecurity; drone forensics is not covered
		China		
Criminal Investigation Police University [81]	Yes	No	Yes	Specialized criminal forensic training; drone forensics underdeveloped

Institution	Digital Forensics	Drone Forensics	Law Enforcement Integration	Comments (Program Offered; aspects of drone forensics)
People's Public Security University [82]	Yes	No	Yes	Strong forensic science programs; no drone evidence focus
Shanghai Jianqiao University [83]	Yes	No	Yes	Master's in Cyberspace Security; drone forensics absent
Zhejiang University [84]	Yes	No	Yes	Graduate cyberspace security; lacks drone-specific research
University of Electronic Science and Technology [85]	Yes	No	Yes	Information & Electronic Forensics; no drone integration
		Saudi Arabia		
NAUSS [12]	Yes	Yes	Yes	Drone evidence specialization; among few comprehensive programs
Prince Sultan Advanced Tech-nol-ogy Research Institute [86]	Yes	Yes	Yes	Drone technology R&D; includes drone forensics
Imam Abdulrahman Bin Faisal University [87]	Yes	No	Yes	Master's in Cybersecurity Forensics; drone forensics not offered
Majmaah University [88]	Yes	No	Yes	Master's in Cybersecurity Forensics; drone forensics not offered
Dar Al-Hekma University [89]	Yes	No	Yes	Bachelor's in Ethical Hacking; drone forensics missing
		Australia		
Flinders University [13]	Yes	No	Yes	Bachelor in Digital Forensics; drone forensics absent
University of Technology Sydney [90]	Yes	No	Yes	Forensic Science with labs; no drone-specific courses
UNSW Canberra [91]	Yes	No	Yes	Master in Digital Forensics; drone evidence not covered
University of the Sunshine Coast [92]	Yes	No	Yes	Accredited master's program; drone forensics missing
Murdoch University [93]	Yes	No	Yes	Comprehensive forensic programs; no drone evidence integration

TABLE A2

Professional Institutions in Digital and Drone Forensics.

Organization	Digital Forensics	Drone Forensics	Law Enforcement Integration	Notes
SANS Institute [14]	Yes	Limited	Yes	Leading DFIR training; GIAC certification; few drone-focused modules
Digital Forensics Associ-ation [94]	Yes	No	Yes	Non-profit; promotes research and pro-fessional development
ACFTI [95]	Yes	Emerging	Yes	Hosts academic conferences; publishes forensics journal
SWGDE [15]	Yes	Yes	Yes	Develops standards and best practices for digital evidence
HTCIA [16]	Yes	No	Yes	Global high-tech crime association for investigators
IACIS [17]	Yes	No	Yes	CFCE certification for digital forensic examiners
NCFTA [96]	Yes	No	Yes	Coordinates private–public cybercrime threat responses
DC3 (DoD) [18]	Yes	Yes	Yes	DoD center for cybercrime investigations and forensics
ADFSL [97]	Yes	No	Yes	Hosts Conference on Digital Forensics, Security and Law