International Journal of Safety and Security Engineering
Vol. 15, No. 11, November, 2025, pp. 2393-2402
Journal homepage: http://iieta.org/journals/ijsse

Extraction of Common Processes of the Investigation Models Proposed in the Drone Forensics Domain

Senan A. M. Alhasan[1,2*], Siti Hajar Othman[1]

[1] Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[2] Department of Computer Science, College of Education for Pure Science, University of Mosul, Mosul 42001, Iraq

Corresponding Author Email: senanadelmawlood@graduate.utm.my

https://doi.org/10.18280/ijsse.151119

Received: 24 September 2025
Revised: 28 October 2025
Accepted: 25 November 2025
Available online: 30 November 2025

Keywords:
drone, drone forensics, unmanned aerial vehicle, design science research

ABSTRACT

A recent development in the field of digital forensics is drone forensic (DF), which involves collecting evidence from drone environments. Nevertheless, DF still suffers from a number of issues and challenges that have recently been discovered. The complexity of DF infrastructures is still a key issue that needs to be resolved. Furthermore, redundancy challenges are important obstacles and constraints in DF investigations. The present study proposes a model called Unified Investigation Processes for Drone Forensics Domain (UIP-DFD) in order to identify the investigation processes commonly involved in the models proposed in the DF domain. Furthermore, this study used the design science research (DSR) approach to design an effective and efficient method for analyzing unmanned aerial vehicle (UAV) evidence, ensuring the evidence is identified, gathered, and analyzed based on recognized DF investigation techniques. UIP-DFD comprises five common investigation processes: i) Identification, ii) Data acquisition, iii) Preservation, iv) Data analysis, and v) Reporting. After conducting a comparative analysis, this study concludes that the NIST digital forensic framework is inadequate for DF. In contrast, the proposed UIP-DFD model integrates drone-specific investigation activities, minimizing redundancy and effectively managing the diversity of evidence from onboard systems, controllers, storage devices, and other digital sources.

1. INTRODUCTION

When doing an investigation in the drone forensic (DF) field, the investigators may encounter tangible evidence remaining in the scene from an unmanned aerial vehicle (UAV), including a drone, radio controls, and server. One of the problems in this realm is that it is difficult to determine the ownership of a confiscated drone [1]. Typically, various digital containers are involved in a UAV flight, which results in some challenges when applying one forensic tool to retrieve all the required data. In some situations, even if it is impossible, or at least very difficult, to acquire a forensic image from among the data saved on the memory of a drone camera without compromising its integrity [2]. This forces investigators into the use of wireless connectivity to carry out a remote forensic imaging procedure [3]. There are various types of embedded data storage containers, some of which may be hidden or have restricted access. This can make it challenging for investigators to obtain digital evidence and identify sources for forensic equipment; for example, the microchip in a flight controller store recorded flight data [4]. Because of the immaturity of the DF field, many problems have remained unresolved and even non-understood, and the literature is still suffering from a lack of dependable techniques for the investigation of drones under forensic conditions [5, 6]. One of the other key issues in this domain is that there is no standardized forensic framework. Consequently, according to the study by Reviriego et al. [7], no proactive forensic viewpoint exists. Moreover, there are still significant unresolved issues, such as the lack of structured procedures and consistent automated methodologies in this domain [8]. Developing a conceptual framework could positively affect the validity and credibility of gathered evidence in the case of a criminal situation and investigations [9]. The current study analyzes the metamodeling development methods that have been proposed by the academic community. According to the findings, the digital forensics field lacks certain methods applicable to the meta-model's development [10]. The existing literature was reviewed to define the problems, and five search engines, i.e., IEEE Explorer, Web of Science, Scopus, Science Direct, and Google Scholar, were used to collect the data required for this study. The search engine keywords used in this research were "drone forensics investigation processes" and "drone forensics investigation model". From among the 1367 resulting publications, 30 papers were selected to be used in this study. An in-depth data analysis showed that the DF domain faces several challenges and issues, including challenges associated with the drone investigation processes [11]. The present study uses the design science research (DSR) approach to design a conceptual model so that it can be applied to the forensic investigation of drones. As a result, this paper proposes the

Unified Investigation Processes for Drone Forensics Domain (UIP-DFD) model using the DSR approach. Extracting common processes provides a foundational framework that helps mitigate the wide range of challenges in DF. Standardized processes reduce redundancy, manage data heterogeneity, and improve data integrity despite technical failures and complex data structures. They also support consistent interpretation, reduce human error, strengthen legal compliance and admissibility, and enable more efficient use of limited resources. Overall, common processes offer a structured and scalable way to address technical, legal, and organizational constraints in DF investigations. The DF domain's research workflow is shown in Figure 1.

The structure of this paper is as follows: Section 1 presents an introduction to the DF domain. Afterward, Section 2 discusses current challenges and issues in this domain. Section 3 introduces the problem identification in the DF domain. Then, Section 4 elaborates on how the proposed UIP-DFD model works. Section 5 presents the results and discussion. Finally, Section 6 introduces the paper's conclusion and future work.

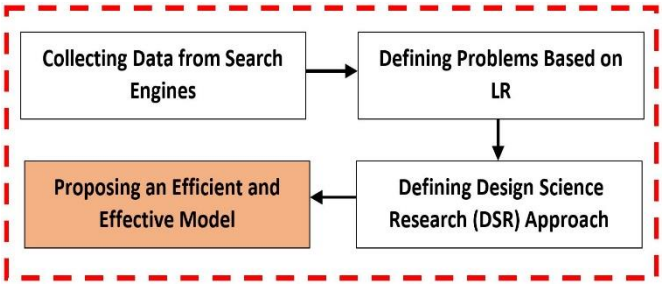

Figure 1. Research workflow in the drone forensic (DF) domain

2. CURRENT CHALLENGES

Several challenges and issues arise because of the distinctive characteristics of drones and the digital data they generate. Figure 2 illustrates the key challenges.

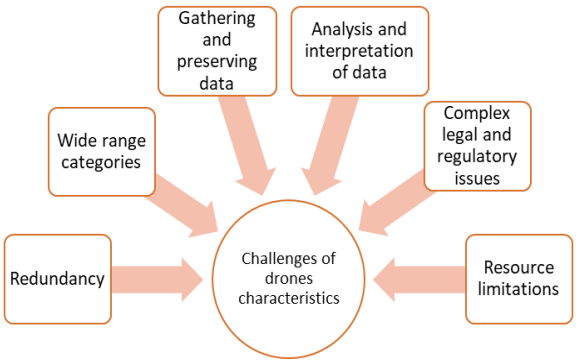

Figure 2. Challenges and issues that arise because of drones' characteristics

Redundancy challenges are important obstacles and constraints in DF investigations. Technical issues that can impede data collecting and processing are just one of these challenges [12, 13]. Technical issues are frequent in drone operations; these issues have arisen because of various factors such as equipment malfunction, signal interference, or software bugs. These kinds of problems can interfere with the drones' flight path, lower the quality of the gathered data, or even result in the whole loss of data. Technical issues not only impede the completion of investigations but also call into question the validity and accuracy of the results. According to Alhussan et al. [14], drone data interpretation demands particular knowledge and proficiency. Finding relevant insights from drone data can be challenging because of its complexity, volume, and diversity. Furthermore, human error, bias, or misinterpretation may occur when interpreting drone data [15]. These limitations highlight the necessity of thorough quality assurance procedures, the participation of professionals who have an in-depth understanding of drone technology, and data interpretation methodologies. Therefore, it is essential to solve redundancy issues in drone investigations to ensure the authenticity and dependability of the acquired data and the accuracy of the interpretations produced based on them [16]. The presence of a wide range of categories is an important challenge in the DF domain. Since drones come in a variety of sizes, configurations, and capabilities, creating standardized forensic methods that work everywhere is challenging. Forensic investigators might have to adapt their methodologies to each type of drone because they may use various communication protocols, storage techniques, and data formats [17]. Gathering and preserving data is not an easy task in DF. Owing to the lack of standardized techniques and tools, extracting data from drones can be complicated. Forensic investigators must ensure that data are gathered and preserved in a forensically sound manner to maintain their integrity and admissibility [18]. For the analysis and interpretation of drones' data, it is important to understand flight patterns, GPS data, sensor readings, and other pertinent data. Retrieval of valuable intelligence and understanding the context of the data might be challenging, especially when handling massive amounts of data or encrypted information [19]. Complex legal and regulatory issues are another challenge in this field. Different countries have different legislation regarding the use of drones. Furthermore, forensic investigators must comprehend and adhere to these intricate guidelines to ensure that their investigations comply with legal criteria and procedures [20]. In addition, the gathering and analysis of data from drones could lead to privacy issues. Another issue that needs to be solved is resource limitations. Specialized tools, equipment, and expertise are frequently required for DF investigation [21]. Resource limitations could impact many law enforcement agencies and digital forensic laboratories, for example, due to limited funding, lack of training, and lack of standardized tools. This affects the access to advanced DF technologies [22].

3. PROBLEM IDENTIFICATION

This research aims to identify an area needed to be further studied in the field of DF and also to explain the reasons and significance that support it. The present paper thoroughly investigates all the pertinent critical research backgrounds. The literature acknowledges the significance, heterogeneity, and complexity of the DF domain. It also recognizes the problem of evidence inconsistency in this field. The challenges regarding evidence inconsistency in drones provide significantly more challenges with technology than traditional computing devices; this is primarily due to the low and small storage of drones. Regardless of whether digital investigators

manage to obtain the drone used in a criminal incident, they occasionally are unable to link it to its owner physically. As the owner is able to dispute their ownership, it must be forensically proven by the investigators [23]. The investigation process now faces a new obstacle that needs to be carefully considered. Numerous investigation facilities and resources might let investigators comprehend in depth a device's entire operation. These resources include the process log files, network log files, and application data from numerous sources. On the other hand, a clear standardization for logging data through various systems has not been offered in the literature yet. Furthermore, gathering data in the most secure possible way is a crucial step in the domain of digital forensics. After that, it is important to assess if the data can be used as evidence in court [24]. Different drones have different methods to connect to the internet. Some drones may only need a cable for the USB port, while others may connect using specific protocols, such as the File Transfer Protocol [25]. In addition, different drone brands have different access permissions that must be provided in order to access the drone. In other words, there are currently no effective techniques for carrying out the process of acquiring drones. For the purpose of addressing these obstacles and learning more about DF, cutting-edge technologies should be combined with the findings of this research as a springboard for gaining a greater understanding of drone infrastructures. In this domain, we may encounter a wide range of devices comprising infrastructures and operational systems. A drone is a device that uses infrastructures and operating systems (OS), which makes DF investigations more complicated since attackers also employ these features in their damaging actions [26]. To determine whether a drone that has been seized had entered a restricted area or not, it is imperative that the flight data be recovered. The problem is that various drones use different techniques to record flight data, and some may not even store such data. Rebuilding the DF investigation could help this case [27]. In other words, anti-forensic techniques, e.g., encryption, are used by criminals in order not to let investigators gain access to the required data. The literature shows that failing to develop organized techniques to assist investigators in handling drone data is one of the most significant challenges in this field [28, 29]. Although the DF domain faces diverse challenges such as legal constraints, resource limitations, and technical complexity, many of these issues originate from the lack of standardized and consistent investigation processes. This study focuses on extracting common investigation processes as a foundational step to reduce methodological fragmentation. A unified process structure can indirectly support legal compliance, improve resource efficiency, and enhance consistency across heterogeneous drone environments.

3.1 Design science research

DSR is an innovative approach to research that has gained increasing popularity in a variety of disciplines over the past several decades. DSR provides scientists with a comprehensive system to develop, test, and refine solutions to complex problems. This is the environment that indeed defines the problem domain where the relevant phenomena are found. The environment may include individuals, groups, and upcoming or currently used technology. This consists of the problems, tasks, objectives, and possibilities that define the requirements as thought of by organization stakeholders. They are positioned in light of the applications, infrastructure, communication architectures, and development capacities of the current technology [30]. Through this approach, the researcher balances problem-solving research with a rigorous data-driven methodology and also intends to provide deeper insights and knowledge to develop innovative artifacts and systems that are useful and effective in those contexts [31]. The knowledge base contains several foundations and methodologies. The body of the literature provides structures, tools, frameworks, foundational theories, methodologies, concepts, and implementations that can be applied to the build phase of a study. In the evaluation phase, methodologies suggest some guidelines that explain how to use the current approaches and principles, which help the researcher achieve accuracy [32] (see Figure 3).

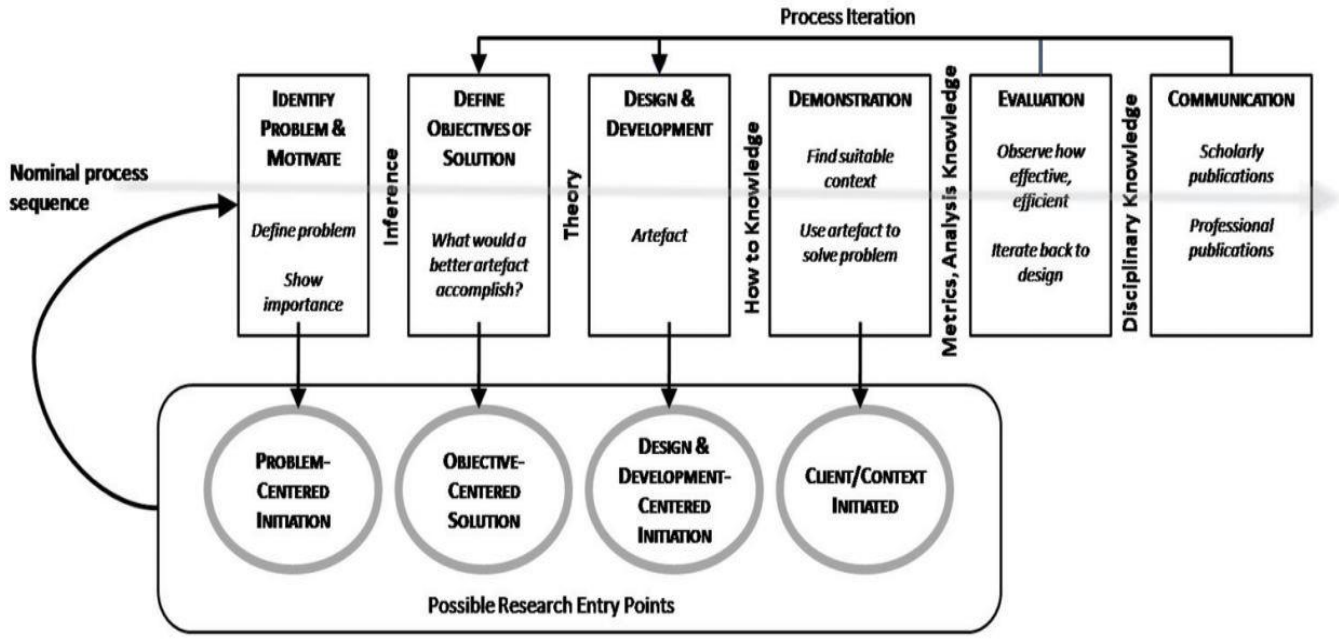

Figure 3. Design science research (DSR) approach [30]

4. METHODOLOGY

In this section, the UIP-DFD model is proposed to solve the heterogeneous, redundant issues and remove irrelevant investigation processes in the DF domain through identifying common investigation processes, as shown in Figure 4.

4.1 Determining drone forensic investigation models

In this step, based on the literature, a set of investigation models is covered. This approach has been adopted by other researchers such as Ameerbakhsh [33] and Alfadli et al. [34]. To fulfill the requirements of the investigation processes in the DF domain, the convergence of concepts and terminologies is extensively applicable. This paper categorizes these DF models based on their perspectives, which include the technologies perspective (algorithm, tool, method) and the investigation processes perspective [35]. As many as 22 models were determined for the purpose of this study (see Table 1).

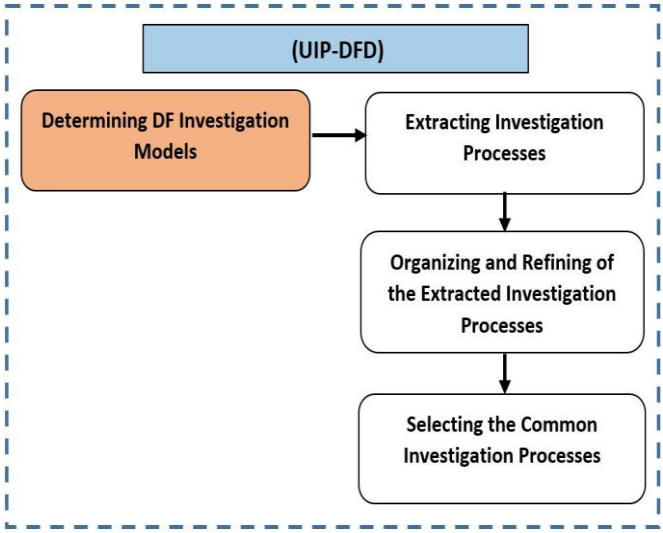

Figure 4. The method proposed in the present research

Table 1. Drone forensic models determined in this study

Models	Year	Title
M1	2022	A comprehensive collection and analysis model for the drone forensics field
M2	2022	An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis
M3	2020	Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0
M4	2023	A conceptual digital forensic investigation model applicable to the drone forensics field
M5	2023	Semantic forensic investigation framework for drone field
M6	2022	A novel forensic readiness framework applicable to the drone forensics field
M7	2022	Unsupervised machine learning for drone forensics through flight path analysis
M8	2022	Drone forensics and machine learning: Sustaining the investigation process
M9	2021	Research challenges and opportunities in drone forensics models
M10	2021	Unmanned aerial vehicle kill chain: Purple teaming tactics
M11	2021	Drone forensics: A case study of digital forensic investigations conducted on common drone models
M12	2020	Drone forensics: A detailed analysis of emerging DJI models
M13	2020	Security analysis of drones' systems: Attacks, limitations, and recommendations
M14	2022	Towards development of a high abstract model for drone forensic domain
M15	2023	Digital forensic research for analyzing drone pilot: Focusing on DJI remote controller
M16	2023	Transformer-based named entity recognition on drone flight logs to support forensic investigation
M17	2021	Drone forensics: A case study on DJI Mavic Air 2
M18	2024	Forensic examination of drones: A comprehensive study of frameworks, challenges, and machine learning applications
M19	2024	Drone forensics: An innovative approach to the forensic investigation of drone accidents based on digital twin technology
M20	2022	Reliable digital forensics in the air: Exploring an rf-based drone identification system
M21	2023	DFLER: Drone Flight Log Entity Recognizer to support forensic investigation on drone device
M22	2025	Drone forensics redefined: Integrating live, digital, and non-digital evidence acquisition systems

4.2 Extracting investigation processes

This step extracts investigation processes from the determined models based on the coverage factors perspective from the related domains [36, 37].

Each model uses a unique set of investigation techniques. For example, the study by Thornton and Zadeh [38] includes 5 investigation processes: *Seized devices*, *Physical examination and planning*, *Extraction*, *Data analysis*, and *Reporting*. On the other hand, the study by Baig et al. [39] includes 4: *Seized devices*, *Data storage*, *Data acquisition*, and *Reporting*. Syed et al. [40] have included 3 investigation processes: *Log flight acquisition*, *Extract log flight*, and *Analyzing flight path*. Finally, Lan and Lee [25] have only 2 investigation processes: *Identification*, and *Scenarios description* (see Table 2 and Figure 5).

Table 2. Extracted investigation processes from the determined model

Models	Extracted Investigation Processes	No. of Processes	References
M1	Data acquisition, Preservation, Reconstruction of the events, Documentation	4	[41]
M2	Seized devices, Physical Examination and Planning, Data Extraction, Data analysis, Reporting	5	[38]
M3	Factory Reset, Scenarios creation, Data acquisition, Testing flight path, Reporting	5	[42]
M4	Testing environment and Equipment, Scenario creation, Data acquisition	3	[43]
M5	Preparation, Data collection, preservation, Reconstructing the events, Documentation	5	[33]
M6	Preparation and monitoring, Preservation, Rehashing data, Documentation, Reporting	5	[37]

M7	Log flight acquisition, Extract log flight, Analyze flight path	3	[40]
M8	Seized devices, Data storage, Data acquisition, Reporting	4	[39]
M9	Pre-incident, Post-incident preparation, Data acquisition, Reconstruct timeline	4	[44]
M10	Identification, Planning, Scenarios description	3	[45]
M11	Identification, Data acquisition, Data analysis, Documentation	4	[28]
M12	Testing environment and equipment, Scenario creation, Data extraction	3	[46]
M13	Preparation, Preservation, Data analysis, Seized devices, Reporting	5	[47]
M14	Identification, Data acquisition, Preservation, Reconstructing timeline	4	[14]
M15	Fixing Equipment, Scenario creation, Data analysis	3	[3]
M16	Data collection, Data examination, Data corrections, Data analysis	4	[2]
M17	Scenarios description, Data acquisition	2	[25]
M18	Gathering evidence, Data analysis, Visualization log file	3	[48]
M19	Identification of suspects, Extraction of artefacts, Interpretation of flight data	3	[18]
M20	Identification, Seized devices, Extraction and analysis, Reporting	4	[49]
M21	Identification, Data acquisition, Preservation, Data analysis	4	[8]
M22	Telemetry logs, Timeline analysis, Replaying log files	3	[50]
Total: 83 investigation processes			

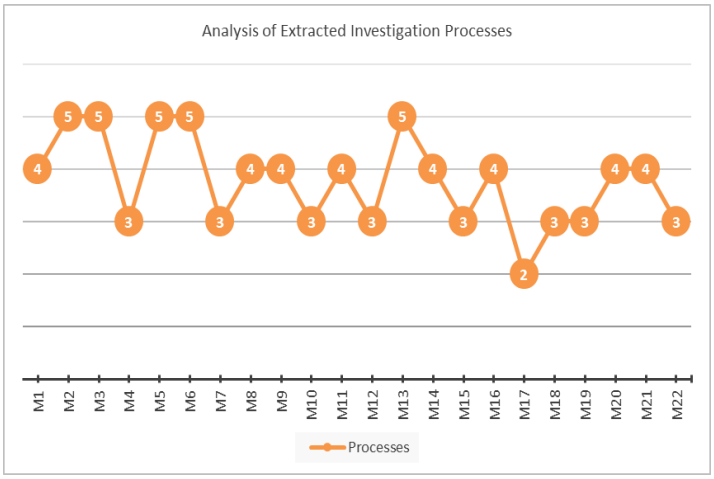

Figure 5. Analysis of extracted investigation processes

4.3 Organizing and refining the extracted investigation processes

In this section, similar investigation processes were identified through semantic and functional analysis, where processes with equivalent objectives, inputs, or forensic outcomes were grouped despite terminological differences across models. Importance was determined based on recurrence frequency across the analyzed models and the process's relevance to maintaining forensic integrity, evidentiary validity, and investigation completeness. This dual criterion ensured that selected processes were both empirically prevalent and conceptually essential to DF. Furthermore, 83 investigation processes from 22 models are organized and refined based on their similar processes and significance to select common investigation processes. Therefore, the extracted processes will be organized to prevent redundancy that frequently confuses practitioners working in the DF domain. This will assist in proposing common investigation processes [41, 42], as shown in Table 3. The first organized and refined investigation process is known as *Identification* process. The *Identification* process proposed by Alhussan et al. [14] is used to identify when the drone has been attacked by any systems, laptops, mobile phones, routers, or radio controllers. Another process of interest is *Preparation* process that is used to prepare for physical drone resources and volatile and non-volatile artifacts [33]. The second organized and refined process is *Data acquisition*. For example, the *Data acquisition* process proposed by Alotaibi et al. [41] acquires both volatile and non-volatile items from the suspect drone, while the *Seized devices* process proposed by Yaacoub et al. [47] isolates devices to prevent remote access that could alter forensic evidence. The third organized and refined process is *Preservation* [33, 37, 47]. Tampering with data, hashing, and data backup must be preserved in order to protect integrity and confidentiality. Add to this some other items such as gathered data, backups, hashes, resources, temporary files, volatile and non-volatile artifacts, logs, and memory recordings. The aim of the preservation process is to guarantee that the captured evidence or logged data are not altered, and also to protect the original logs and data with the aid of forensic tools. The process of *Data examination* proposed by Kao et al. [21] is used to identify and preserve the file types that might be relevant to the incident. This process is crucial to law enforcement. The fourth organized and refined process is *Data analysis*. The *Data analysis* proposed by Thornton and Zadeh [38] is used to analyze drone data to create relationships between the devices and provide responsibility to the owner or user of the device. On the other hand, the *Reconstruct timelines* process proposed by the previous studies [14, 44] is used to piece together the drone's timeline and expose the evidence of the crime. The accuracy of the reconstructed event occurrence is the foundation for event sequences in an investigation. The fifth process identified in this study was *Reporting*, proposed by the previous research [42, 49]. The final phase in digital forensics provides a report of the investigation's results, accompanied by evidence of the devices' usage in criminal activities, and distributes it to the

relevant custody. Finally, *Documentation* process was identified, which was proposed by Al-Room et al. [28]. Investigators need to document their investigation in such a way that it could benefit DF experts and/or courts.

Table 3. Organized processes and the common processes selected across all models

Processes	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11	M 12	M 13	M 14	M 15	M 16	M 17	M 18	M 19	M 20	M 21	M 22	Category
★Identification										√	√			√					√	√	√		Nominee
Preparation					√								√										Equivalent
Preparation and monitoring						√																	Equivalent
Incident response														√									Equivalent
Physical examination and Planning		√																					Equivalent
Planning										√													Equivalent
Pre-incident preparation									√														Equivalent
Post-incident preparation									√														Equivalent
Factory reset			√																				Equivalent
Testing environment and equipment				√								√											Equivalent
Scenarios creation			√	√								√			√								Equivalent
Scenarios description										√													Equivalent
Models	**M 1**	**M 2**	**M 3**	**M 4**	**M 5**	**M 6**	**M 7**	**M 8**	**M 9**	**M 10**	**M 11**	**M 12**	**M 13**	**M 14**	**M 15**	**M 16**	**M 17**	**M 18**	**M 19**	**M 20**	**M 21**	**M 22**	**Category**
★Data acquisition	√		√	√				√	√		√			√			√				√		Nominee
Data collection					√											√				√			Equivalent
Data gathering					√																		Equivalent
Seized devices		√						√					√							√			Equivalent
Log flight acquisition							√																Equivalent
Gathering evidence																		√					Equivalent
Telemetry logs																						√	Equivalent
Data extraction		√										√											Equivalent
Extract log flight							√																Equivalent
Extraction of artefacts																			√				Equivalent
Models	**M 1**	**M 2**	**M 3**	**M 4**	**M 5**	**M 6**	**M 7**	**M 8**	**M 9**	**M 10**	**M 11**	**M 12**	**M 13**	**M 14**	**M 15**	**M 16**	**M 17**	**M 18**	**M 19**	**M 20**	**M 21**	**M 22**	**Category**
★Preservation	√				√	√							√	√							√		Nominee
Data examination																√							Equivalent
Fixing equipment															√								Equivalent
Telemetry logs																						√	Equivalent
Visualization log file																		√					Equivalent
Models	**M 1**	**M 2**	**M 3**	**M 4**	**M 5**	**M 6**	**M 7**	**M 8**	**M 9**	**M 10**	**M 11**	**M 12**	**M 13**	**M 14**	**M 15**	**M 16**	**M 17**	**M 18**	**M 19**	**M 20**	**M 21**	**M 22**	**Category**
★Data analysis		√									√		√		√	√		√			√		Nominee
Reconstructing event	√	√			√				√											√			Equivalent
Reconstructing timeline									√					√				√				√	Equivalent
Reconstructing scene											√												
Testing flight path			√																				Equivalent
Flight path analysis							√																Equivalent
Replaying log files																						√	Equivalent
Flight path scenario				√																			
Extraction and analysis																				√			Equivalent
Rehashing data						√																	Equivalent
Interpretation of flight data																			√				Equivalent
Timeline analysis									√													√	Equivalent
Models	**M 1**	**M 2**	**M 3**	**M 4**	**M 5**	**M 6**	**M 7**	**M 8**	**M 9**	**M 10**	**M 11**	**M 12**	**M 13**	**M 14**	**M 15**	**M 16**	**M 17**	**M 18**	**M 19**	**M 20**	**M 21**	**M 22**	**Category**
★Reporting		√	√			√		√					√							√			Nominee
Documentation	√				√	√					√												Equivalent

Note: ★ indicates the selected processes.

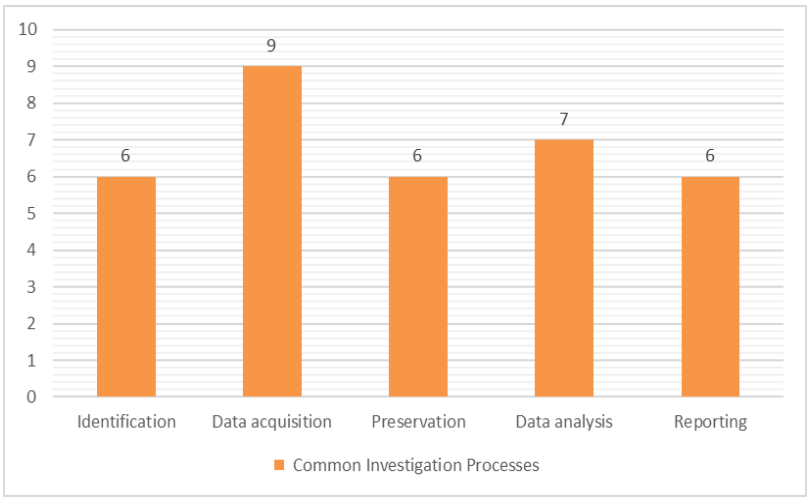

Figure 6. The common investigation processes proposed in this study

4.4 Selecting the common investigation processes

After organizing and refining the extracted investigation processes, the processes that had a higher frequency were selected for the investigation process. Among all the extracted processes, and nominee five more common investigation processes were identified: *Identification*, *Data acquisition, Preservation, Data analysis,* and *Reporting,* as shown in Table 3. The *Identification* process identifies all the necessary resources for the investigation, including the investigation team, incident response strategies, reliable forensic tools, and sources to be seized. The *Data acquisition* process is used to collect and gather the whole drone data, including volatile and non-volatile data. The *Preservation* process protects the data that has been gathered, i.e., backups, hashes, resources, temporary files, and volatile/non-volatile artifacts. The *Data analysis* process is used to reconstruct timeline events, analyze these incidents, and find the criminal. Finally, the *Reporting* process prepares the final evidence for the full digital forensic analysis. Forensic experts use this evidence report when they witness in a court of law.

The investigative method was chosen as a typical investigation process because it occurs frequently in categorization. Five typical processes were identified in this study: *Identification, Data acquisition, Preservation, Data analysis,* and *Reporting*. They were selected from among 22 models identified in the literature (see Table 3).

The *Identification* process appeared in six different models: M10, M11, M14, M19, M20, and M21.

The *Data acquisition* process appeared in nine different models: M1, M3, M4, M8, M9, M11, M14, M17, and M21.

The *Preservation* process appeared in six different models: M1, M5, M6, M13, M14, and M21.

The *Data analysis* appeared in seven different models: M2, M11, M13, M15, M16, M18, and M21.

Finally, the *Reporting* process appeared in six different models: M2, M3, M6, M8, M13, and M20. Table 3 presents the organized and refined processes and the five processes selected based on frequency. The proposed common investigation processes are illustrated in Figure 6.

5. RESULTS AND DISCUSSION

The current paper identifies investigation processes commonly used in the DF field. Then, the UIP-DFD model was proposed in this paper in a way that is well applicable to the DF domain. This study presented a comprehensive framework for investigation processes in this domain. The models extracted from the literature were reviewed, and five common investigation processes among 83 extracted investigation processes were identified regarding their frequency: *Identification, Data acquisition, Preservation, Data analysis, and Reporting.* It was done through careful harmonization and consolidation, which ensures a streamlined and efficient approach to conducting investigations in the DF domain.

These processes represent the minimum invariant workflow required for DF investigations and reduce redundancy by consolidating overlapping activities. Moreover, their abstraction addresses platform heterogeneity and supports legal admissibility through structured evidence handling and reporting. Table 4 demonstrates that although the NIST digital forensic framework offers general investigative guidance, its lack of support for distributed UAV data sources, volatile flight telemetry, and particular legal constraints makes it inadequate for DF. In contrast, the proposed UIP-DFD model reduces redundancy and manages heterogeneity across onboard, controller, and digital evidence by unifying drone-related investigation activities.

Table 4. Comparison of the NIST framework and the proposed model

Phase	NIST	UIP-DFD
Scope and applicability	A general framework designed for use with traditional digital devices, and operates linearly	A specialized framework designed for DF, addressing UAV heterogeneity, distributed data sources, and redundancy in forensic processes
Handling of heterogeneity	Assumes relatively homogeneous devices and centralized data sources	Addresses heterogeneous drone platforms, distributed onboard controller devices, and cloud data
Redundancy management	Does not explicitly address process redundancy across specialized DF models	Integrates redundant drone investigative tasks into unified core processes

6. CONCLUSIONS

In this paper, we identified common investigation processes to address the heterogeneous and redundant issues in the DF domain. The relevant models were identified based on extracted criteria. As many as 83 investigation processes were extracted from 22 models. These models were organized and refined based on their similar processes and their significance in order to identify the processes of the highest frequency. As a result, the proposed model comprises five common investigation processes: *Identification, Data acquisition, Preservation, Data analysis,* and *Reporting*. The proposed UIP-DFD model can help DF researchers, investigators, and stakeholders to manage, re-share, and organize the tasks related to their investigations. For future research, authors can use the proposed UIP-DFD to identify common investigation concepts of DF, as well as develop a comprehensive model known as a meta-model.

ACKNOWLEDGMENT

The authors would like to acknowledge the Ministry of Higher Education Malaysia and the Universiti Teknologi Malaysia (Vote: R.J130000.7851.5F566) for funding this research under the Fundamental Research Grant Scheme (Grant No.: FRGS/1/2022/ICT07/UTM/02/1).

REFERENCES

[1] Horsman, G. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. Digital Investigation, 16: 1-11. https://doi.org/10.1016/j.diin.2015.11.002

[2] Silalahi, S., Ahmad, T., Studiawan, H. (2023). Transformer-based named entity recognition on drone flight logs to support forensic investigation. IEEE Access, 11: 3257-3274. https://doi.org/10.1109/ACCESS.2023.3234605

[3] Lee, S., Seo, H., Kim, D. (2023). Digital forensic research for analyzing drone pilot: Focusing on DJI remote controller. Sensors, 23(21): 8934. https://doi.org/10.3390/s23218934

[4] Rezaee, M.R., Hamid, N.A.W.A., Hussin, M., Zukarnain, Z.A. (2024). Comprehensive review of drones collision avoidance schemes: Challenges and open issues. IEEE Transactions on Intelligent Transportation Systems, 25(7): 6397-6426. https://doi.org/10.1109/TITS.2024.3375893

[5] Sibe, R.T., Bekom, D. (2025). 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, 15(1): 197-210. https://doi.org/10.54216/JCIM.150115

[6] Lew, R., Ptasznik, B., Wolfer, S. (2024). The effectiveness of ChatGPT as a lexical tool for English, compared with a bilingual dictionary and a monolingual learner's dictionary. Humanities and Social Sciences Communications, 11(1): 1-10. https://doi.org/10.1057/s41599-024-03775-y

[7] Reviriego, P., Conde, J., Merino-Gómez, E., Martínez, G., Hernández, J.A. (2024). Playing with words: Comparing the vocabulary and lexical richness of ChatGPT and humans. Machine Learning with Applications, 18: 100602. https://doi.org/10.1016/j.mlwa.2024.100602

[8] Silalahi, S., Ahmad, T., Studiawan, H. (2023). DFLER: Drone Flight Log Entity Recognizer to support forensic investigation on drone device. Software Impacts, 15: 100457. https://doi.org/10.1016/j.simpa.2022.100457

[9] Bade, A.M., Othman, S.H. (2022). Towards adapting metamodelling technique for an Online Social Networks Forensic Investigation (OSNFI) domain. International Journal of Advanced Computer Science and Applications, 13(7): 166-173. https://doi.org/10.14569/IJACSA.2022.0130722

[10] Ameerbakhsh, O., Ghabban, F.M., Alfadli, I.M., AbuAli, A.N., Al-Dhaqm, A., Al-Khasawneh, M.A. (2021). Digital forensics domain and metamodeling development approaches. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, pp. 67-71. https://doi.org/10.1109/ICSCEE50312.2021.9497935

[11] Alhasan, S.A., Othman, S.H., Al-Dhaqm, A. (2025). Metamodeling-based drone forensics investigation: A systematic literature review. International Journal of Safety & Security Engineering, 15(1): 1-12. https://doi.org/10.18280/ijsse.150101

[12] Sharma, S., Sharma, H. (2024). Drone a technological leap in health care delivery in distant and remote inaccessible areas: A narrative review. Saudi Journal of Anaesthesia, 18(1): 95-99. https://doi.org/10.4103/sja.sja_506_23

[13] Velusamy, P., Rajendran, S., Mahendran, R.K., Naseer, S., Shafiq, M., Choi, J.G. (2022). Unmanned aerial vehicles (UAV) in precision agriculture: Applications and challenges. Energies, 15(1): 217. https://doi.org/10.3390/en15010217

[14] Alhussan, A.A., Al-Dhaqm, A., Yafooz, W.M., Razak, S.B.A., Emara, A.H.M., Khafaga, D.S. (2022). Towards development of a high abstract model for drone forensic domain. Electronics, 11(8): 1168. https://doi.org/10.3390/electronics11081168

[15] Lau, Y.H., Ang Jr, M.H. (2021). A novel link failure detection and switching algorithm for dissimilar redundant UAV communication. Drones, 5(2): 48. https://doi.org/10.3390/drones5020048

[16] Bebortta, S., Dalabehera, A.R., Pati, B., Panigrahi, C.R., Nanda, G.R., Sahu, B., Senapati, D. (2022). An intelligent spatial stream processing framework for digital forensics amid the COVID-19 outbreak. Smart Health, 26: 100308. https://doi.org/10.1016/j.smhl.2022.100308

[17] Georgiou, A., Masters, P., Johnson, S., Feetham, L. (2022). UAV-assisted real-time evidence detection in outdoor crime scene investigations. Journal of Forensic Sciences, 67(3): 1221-1232. https://doi.org/10.1111/1556-4029.15009

[18] Almusayli, A., Zia, T., Qazi, E.U.H. (2024). Drone forensics: An innovative approach to the forensic investigation of drone accidents based on digital twin technology. Technologies, 12(1): 11. https://doi.org/10.3390/technologies12010011

[19] Barton, T.E.A., Azhar, M.A.H.B. (2018). Open source forensics for a multi-platform drone system. In

International Conference on Digital Forensics and Cyber Crime, pp. 83-96. https://doi.org/10.1007/978-3-319-73697-6_6

[20] Mantas, E., Patsakis, C. (2022). Who watches the new watchmen? The challenges for drone digital forensics investigations. Array, 14: 100135. https://doi.org/10.1016/j.array.2022.100135

[21] Kao, D.Y., Chen, M.C., Wu, W.Y., Lin, J.S., Chen, C.H., Tsai, F. (2019). Drone forensic investigation: DJI spark drone as a case study. Procedia Computer Science, 159: 1890-1899. https://doi.org/10.1016/j.procs.2019.09.361

[22] Al-Dhaqm, A., Abd Razak, S., Ikuesan, R.A., Kebande, V.R., Siddique, K. (2020). A review of mobile forensic investigation process models. IEEE Access, 8: 173359-173375. https://doi.org/10.1109/ACCESS.2020.3014615

[23] Lin, C.M., Lin, I.L. (2024). Digital forensics according to International Organization for Standardization/International Organization for Standardization 27050 and digital evidence forensics standard operating procedure: Use of Sensor Technology. Sensors & Materials, 36(6): 2315-2324. https://doi.org/10.18494/SAM4871

[24] Mohamed, H., Koroniotis, N., Schiliro, F., Moustafa, N. (2025). IoT-CAD: A comprehensive Digital Forensics dataset for AI-based Cyberattack Attribution Detection methods in IoT environments. Ad Hoc Networks, 174: 103840. https://doi.org/10.1016/j.adhoc.2025.103840

[25] Lan, J.K.W., Lee, F.K.W. (2022). Drone forensics: A case study on DJI Mavic Air 2. In 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea, pp. 291-296. https://doi.org/10.23919/ICACT53585.2022.9728844

[26] Pathania, A., Gangwar, D.P., Shivanshu, P., Angrish, A. (2021). Unmanned aerial vehicle forensic investigation process: Dji Phantom 4 drone as a case study. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(4): 593-599. https://doi.org/10.32628/CSEIT2174136

[27] Kuforiji, J. (2025). Digital Forensics and Incident Response (DFIR) automation: Leveraging AI to accelerate breach investigation, evidence collection, and cyberattack mitigation. Journal of Data Analysis and Critical Management, 1(4): 1-19. https://doi.org/10.64235/tsvfvz27

[28] Al-Room, K., Iqbal, F., Baker, T., Shah, B., Yankson, B., MacDermott, A., Hung, P.C. (2021). Drone forensics: A case study of digital forensic investigations conducted on common drone models. International Journal of Digital Crime and Forensics (IJDCF), 13(1): 1-25. https://doi.org/10.4018/IJDCF.2021010101

[29] Saleh, M.A., Othman, S.H., Al-Dhaqm, A., Al-Khasawneh, M.A. (2021). Common investigation process model for Internet of Things forensics. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, pp. 84-89. https://doi.org/10.1109/ICSCEE50312.2021.9498045

[30] Calvetti, D., Mêda, P., Hjelseth, E., de Sousa, H. (2025). Incremental digital twin framework: A design science research approach for practical deployment. Automation in Construction, 170: 105954. https://doi.org/10.1016/j.autcon.2024.105954

[31] Al-Dhaqm, A., Abd Razak, S., Othman, S.H., Nagdi, A., Ali, A. (2016). A generic database forensic investigation process model. Jurnal Teknologi (Sciences & Engineering), 78(6-11): 45-57. https://doi.org/10.11113/jt.v78.9190

[32] Henriques, T.A., O'Neill, H. (2023). Design science research with focus groups–a pragmatic meta-model. International Journal of Managing Projects in Business, 16(1): 119-140. https://doi.org/10.1108/IJMPB-01-2020-0015

[33] Ameerbakhsh, O. (2023). Semantic forensic investigation framework for drone field. Journal of Computer Science, 19(2): 212-228. https://doi.org/10.3844/jcssp.2023.212.228

[34] Alfadli, I.M., Ghabban, F.M., Ameerbakhsh, O., AbuAli, A.N., Al-Dhaqm, A., Al-Khasawneh, M.A. (2021). Cipm: Common identification process model for database forensics field. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, pp. 72-77. https://doi.org/10.1109/ICSCEE50312.2021.9498014

[35] Saleh, M., Othman, S.H., Driss, M., Al-dhaqm, A., Ali, A., Yafooz, W.M., Emara, A.H.M. (2023). A metamodeling approach for IoT forensic investigation. Electronics, 12(3): 524. https://doi.org/10.3390/electronics12030524

[36] Thallapureddy, S., Sherratt, F., Hallowell, M., Bhandari, S. (2024). Effective information collection in incident investigations: A systematic review and narrative synthesis. Safety Science, 171: 106404. https://doi.org/10.1016/j.ssci.2023.106404

[37] Alotaibi, F.M., Al-Dhaqm, A., Al-Otaibi, Y.D. (2022). A novel forensic readiness framework applicable to the drone forensics field. Computational Intelligence and Neuroscience, 2022(1): 8002963. https://doi.org/10.1155/2022/8002963

[38] Thornton, G., Zadeh, P.B. (2022). An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis. Forensic Science International: Digital Investigation, 41: 301379. https://doi.org/10.1016/j.fsidi.2022.301379

[39] Baig, Z., Khan, M.A., Mohammad, N., Brahim, G.B. (2022). Drone forensics and machine learning: Sustaining the investigation process. Sustainability, 14(8): 4861. https://doi.org/10.3390/su14084861

[40] Syed, N., Khan, M.A., Mohammad, N., Brahim, G.B., Baig, Z. (2022). Unsupervised machine learning for drone forensics through flight path analysis. In 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, pp. 1-6. https://doi.org/10.1109/ISDFS55398.2022.9800808

[41] Alotaibi, F.M., Al-Dhaqm, A., Al-Otaibi, Y.D., Alsewari, A.A. (2022). A comprehensive collection and analysis model for the drone forensics field. Sensors, 22(17): 6486. https://doi.org/10.3390/s22176486

[42] Bouafif, H., Kamoun, F., Iqbal, F. (2020). Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0. International Journal of Digital Crime and Forensics (IJDCF), 12(1): 35-57. https://doi.org/10.4018/IJDCF.2020010103

[43] Alotaibi, F., Al-Dhaqm, A., Al-Otaibi, Y.D. (2023). A conceptual digital forensic investigation model applicable to the drone forensics field. Engineering, Technology & Applied Science Research, 13(5): 11608-

11615. https://doi.org/10.48084/etasr.6195
[44] Al-Dhaqm, A., Ikuesan, R.A., Kebande, V.R., Razak, S., Ghabban, F.M. (2021). Research challenges and opportunities in drone forensics models. Electronics, 10(13): 1519. https://doi.org/10.3390/electronics10131519
[45] Salamh, F.E., Karabiyik, U., Rogers, M.K., Matson, E.T. (2021). Unmanned aerial vehicle kill chain: Purple teaming tactics. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, pp. 1081-1087. https://doi.org/10.1109/CCWC51732.2021.9376090
[46] Yousef, M., Iqbal, F., Hussain, M. (2020). Drone forensics: A detailed analysis of emerging DJI models. In 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, pp. 66-71. https://doi.org/10.1109/ICICS49469.2020.239530
[47] Yaacoub, J.P., Noura, H., Salman, O., Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11: 100218. https://doi.org/10.1016/j.iot.2020.100218
[48] Debas, E.A., Albuali, A., Rahman, M.H. (2024). Forensic examination of drones: A comprehensive study of frameworks, challenges, and machine learning applications. IEEE Access, 12: 111505-111522. https://doi.org/10.1109/ACCESS.2024.3426028
[49] Li, Z.X., Chen, B.C., Chen, X.Y., Xu, C.H., et al. (2022). Reliable digital forensics in the air: Exploring an RF-based drone identification system. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 6(2): 63. https://doi.org/10.1145/3534598
[50] Lee, D., Kang, W. (2025). Drone forensics redefined: Integrating live, digital, and non-digital evidence acquisition systems. Forensic Science International: Synergy, 11: 100635. https://doi.org/10.1016/j.fsisyn.2025.100635