electronics

MDPI

Article

Towards Development of a High Abstract Model for Drone Forensic Domain

Amel Ali Alhussan [1], Arafat Al-Dhaqm [2], Wael M. S. Yafooz [3], Shukor Bin Abd Razak [2], Abdel-Hamid M. Emara [3,4] and Doaa Sami Khafaga [1,*]

1 Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; aalhussan@pnu.edu.sa
2 Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia (UTM), Johor Skudai 813110, Malaysia; mrarafat1@utm.my (A.A.-D.); shukorar@utm.my (S.B.A.R.)
3 Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia; wyafooz@taibahu.edu.sa (W.M.S.Y.); aemara@taibahu.edu.sa (A.-H.M.E.)
4 Department of Computers and Systems Engineering, Faculty of Engineering, Al-Azhar University, Cairo 11884, Egypt
* Correspondence: dskhafga@pnu.edu.sa

Abstract: Drone Forensics (DRF) is one of the subdomains of digital forensics, which aims to capture and analyse the drone's incidents. It is a diverse, unclear, and complex domain due to various drone field standards, operating systems, and infrastructure-based networks. Several DRF models and frameworks have been designed based on different investigation processes and activities and for the specific drones' scenarios. These models make the domain more complex and unorganized among domain forensic practitioners. Therefore, there is a lack of a generic model for managing, sharing, and reusing the processes and activities of the DRF domain. This paper aims to develop A Drone Forensic Metamodel (DRFM) for the DRF domain using the metamodeling development process. The metamodeling development process is used for constructing and validating a metamodel and ensuring that the metamodel is complete and consistent. The developed DRFM consists of three main stages: (1) identification stage, (2) acquisition and preservation stage, and (3) examination and data analysis stage. It is used to structure and organize DRF domain knowledge, which facilitates managing, organizing, sharing, and reusing DRF domain knowledge among domain forensic practitioners. That aims to identify, recognize, extract and match different DRF processes, concepts, activities, and tasks from other DRF models in a developed DRFM. Thus, allowing domain practitioners to derive/instantiate solution models easily. The consistency and applicability of the developed DRFM were validated using metamodel transformation (vertical transformation). The results indicated that the developed DRFM is consistent and coherent and enables domain forensic practitioners to instantiate new solution models easily by selecting and combining concept elements (attribute and operations) based on their model requirement.

Keywords: drone forensic; metamodel; metamodeling; metamodel transformation; UAV

Citation: Alhussan, A.A.; Al-Dhaqm, A.; Yafooz, W.M.S.; Razak, S.B.A.; Emara, A.-H.M.; Khafaga, D.S. Towards Development of a High Abstract Model for Drone Forensic Domain. *Electronics* **2022**, *11*, 1168. https://doi.org/10.3390/electronics11081168

Academic Editors: Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis, Thomas Lagkas and Vasileios Argyriou

Received: 16 February 2022
Accepted: 25 March 2022
Published: 7 April 2022

1. Introduction

The DRF domain is a well-known and significant field that collects, identifies, and reconstructs the documents related to potential UAV incidents [1]. Several models, frameworks, methods, approaches, tools, and algorithms have been offered for the DRF domain in the literature to deal with different UAV incidents. Nevertheless, there is still a lack of a structured and unified model to manage, facilitate, share, and reuse the DRF tasks and activities among domain forensic practitioners [2]. Therefore, this study aims to develop Drone Forensic Metamodel (DRFM) using the metamodeling process approach. The metamodeling development process is used for constructing and validating a metamodel [3]. The metamodeling development process ensures that the metamodel is complete and

consistent [3]. The metamodel consists of three levels, as shown in Figure 1: M2-Level, M1-Level, and M0-Level. The M2-Level is the high abstract level called metamodel or meta-meta data, which is used to govern the behaviors of the M1-Level. The M1-Level is the metadata level or user model, which is the domain model and is used to control the behavior of the M0-Level. The M0-Level is the data level or the user data model, which deals with the actual domain data. Therefore, the primary purpose of this paper is to develop a metamodel (M2-Level) for the DRF domain to govern, structure, organize, unify, and manage DRF knowledge. The objectives of this paper are as follow:

- Discussing the existing challenges and issues related to the DRF domain
- Developing a high abstract model (DRFM) using a metamodeling approach
- Validating the developed DRFM

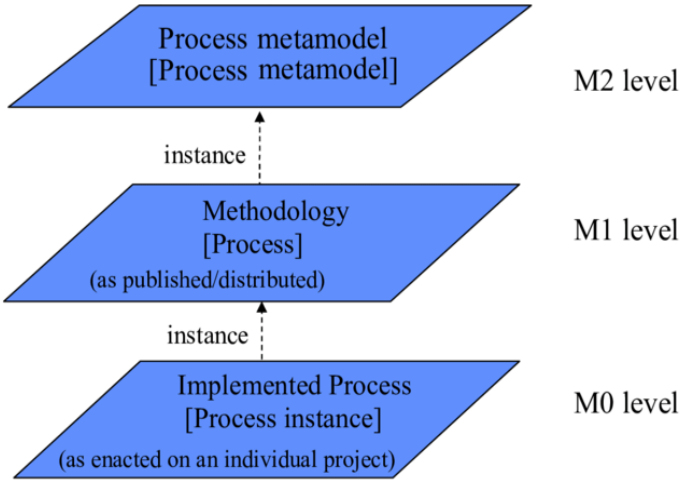

Figure 1. Metamodel layers [4].

This study contributes to the solution of the interoperability, heterogeneity, and complexity issues of the DRF domain through the proposal of a new structured and unified metamodel (DRFM) that facilitates structuring, organizing, sharing, managing, and reusing DRF domain knowledge. Moreover, the study is an explicit artifact to describe DRF knowledge among domain forensic practitioners. This research can not only assist domain practitioners (incident responders, examiners, investigators, and analyzers) in the development of solution models for their problems but can also provide insight into how to promote the newcomers to use this metamodel as a guideline to investigate drone incidents.

The remaining parts of the paper are organized as follows. Section 2 presents the related work and research methodology to design the proposed model discussed in Section 3. Section 4 offers and discusses the findings. Finally, Section 5 concludes the paper and recommends directions for future research.

2. Related Works

Several works have been introduced for the DRF domain in the literature. However, the existing work discussed the DRF domain from a technical perspective. For example, [5,6] discussed the processes to recover the required evidence for digital forensics examined the processes to recover the required evidence for digital forensics. These solutions have focused on the wireless aspects of forensics. In [6], the authors concentrated on all parts of UAVs. Their focus is on the operating system (Linux) and its desirable features for the data collection as evidence for forensics. The authors in [5] applied a particular tool (Java-FX) to real-time visualization and flight control. This kind of tool cannot be directly deployed due to the relationship between drone nodes and controllers for data communication processes. This tool is also used to visualize the sensor parameters such as GPS, IMU, and altitude for flight safety and protection. Similarly, in [7], the authors analyzed forensically the DJI Phantom 2 Vision Plus to answer the following critical question: "Can the flight

path of a UAV be reconstructed with the use of positional data collected from a UAV?". Additionally, the authors used an investigation method to counter the forensic examination whenever the flight path was recorded and detected. In another study [8], the researchers performed a preliminary forensic analysis on the Parrot Bebop. The Parrot Bebop is comparable with Parrot AR Drone 2.0. The authors also addressed the UAVs forensics key issues. Their investigation was divided into two separate parts: flight controller and UAV. The ".pud" file was used for data retrieval from the device. A new ".pud" file is formed when the session initiates between UAV and controller. A set of metadata is observed at the start of the ".pud" file, a serial number of the UAV, time and date of flight, controller model, and the application used for flight control. After this, the multimedia data (including video and audio) are identified and recorded by UAVs onboard camera. The latitude and longitude data extracted from images and EXIF data are used to record the coordinates of the places. When the controller and UAV are seized using the identification and the serial number of the device, the ownership could be established. The authors in [9] discussed the DRF and usage of DJI Phantom 2. The authors also conducted the breakdown analysis of software and hardware components of UAVs and methods used for implementing DRF. Their study also provided a proper platform to improve and scrutinize the DRF concept. In another study [10], the researchers discussed the visualizing and integration of data retrieved from UAV nodes and applied a non-forensic method. The authors used Parrot AR Drone 2.0 and a customized self-made application in which the log parameters of flight are visualized. However, this evaluation has been conducted on only a few numbers of drones. In [11], the authors discussed the susceptibilities and usage of drones and their relationships with cybercrime and security issues. Their findings revealed that the cases of drone hacking cause ramifications and threats. They also concluded that the drones have an extensive range, where small drones (toys) could be adopted as a weapon for mass destruction. The authors in [12] designed a forensic framework comprising 12 phases, through which UAVs could be investigated systematically. The authors also investigated five commercial UAVs to check the relationship of different components. They used Parrot AR Drone 2.0 for the experiments required. In addition, they validated the proposed framework. Every UAV node was tested and modified using the addition and removal of the components. This effort was done to determine the main factors and elements involved in commercial UAVs test for analysis. It was concluded that the absence of law enforcement is one of the critical challenges and weaknesses of the existing systems. In [13], the first wide-range analysis of the DJI Phantom 3 standard was carried out. The authors also used the Drone Open-Source Parser (DROP) tool for forensic analysis. The acquired data were divided into three parts: drone, controller, and phone or tablet. The two types of files were explored, i.e., ".dat" and ".txt" generated from the DJI GO tool. Both files were processed and decoded/decrypted. The information was related to GPS location information, Wi-Fi connections, flight status, motors, and remote control. After this process, the DROP tool was used for the proprietary file structures for analysis. Also, the authors discussed the UAV turn-on position status where the integrity of data is kept for internal storage. A New .dat file is generated whenever the UAV turns on. Furthermore, it was also observed that SD cards are placed near UAVs and extract data immediately. The researchers in [14] discussed the GPS coordinates applied as location evidence during crime investigations. They also extracted the system logs and made the visualization of GPS coordinates on maps. The third-party web-based platforms were employed to plot the flight path. In [14], the authors presented a forensic model for drone components authentication employed with unlawful deeds. The authors also emphasized the physical evidence analysis performed on the crime scene along with GPS-related data or multimedia data found on board. They used five drone types that were seized at crime scenes. They identified two key issues: drone attacks and the shortage of law enforcement training processes. In [15], the focus was placed on the impact of quadcopter's downwash to determine the effect of retention of the evidence from crime scenes. In [16], the authors discussed the correlation of the flight data by using mobile devices or SD cards. The authors also examined the link

between drones and suspects and their facilitating factors. The native OS or software was used to protect the UAVs. They also highlighted the GPS, distance, timestamps and waypoints, roll, the number of satellites connected, barometer, pitch, distance, battery status, azimuth, video, and photos. In [17], the researchers analyzed the significant log parameters for UAVs and suggested the software architecture. The software should be user-friendly and able to extract on-board flight information. They expected that the toll would be helpful for forensic investigation and drone-related crime cases. In [17], the author presented open-source tools such as CSV-View and ExifTool for artifacts extraction. Geo-player as an open-source tool was used to visualize flight path data. Due to the nonexistence of any feasible tool in the UAV system, they needed to package manager or compiler in the UAV nodes. Digital forensics was applied to the Parrot A.R Drone 2.0, and various files format and facts were discussed. With the use of Google Earth, the flight paths were visualized. In [18], the authors analyzed the in-depth forensics applied to Parrot AR Drone 2.0 and flight recorder and flight controller. In [19], the authors explored the difficulties in forensically analyzing UAVs/drones. The authors decided that there is a need for a guideline for drone forensics. After this gap analysis, the authors suggested the guidelines based on existing policies and guidelines. In [20], the authors proposed an architecture based on the Id-Based Signcryption to guarantee the authentication process and privacy preservation. The authors defined the essential elements of architecture and then discussed the interaction between these elements to understand the processes. The authors used RFID tags for drone tracking purposes and ensured the drone's privacy. The simulation results indicated the average renewal of temporary identity by varying the drone speed and time. In [21], the authors presented UAV forensic conditions where the suspected UAV was captured from the side of the forces or crashed into private property. There is a need to identify the used hardware or software for drone forensic investigations and collect the available evidence. In aviation regulation, it is observed that the illegitimate usage of UAVs is a legal loophole. This leads to the weakness of existing standards to handle UAV incidents. In [22], the authors discussed the cyber-physical security issues related to UAVs and their threats to smart cities. The authors also suggested a method applicable to the large-scale cyber security attacks vectors. These systems are categorized into four systems for the operations of UAVs. In [23], furthermore, the authors elaborated on the impact and effective ways to tackle existing or new attacks. In another effort, in [24], the authors discussed an inclusive architecture for drone forensic investigations, for both digital and physical forensics. Their proposed framework was capable of performing post-flight investigations and other related activities. For physical forensics, a model was designed for drone investigation, where the drone components are examined at the crime scene. The authors also presented an application that could perform drone forensic analyses and check the drone's critical log parameters by using the GUI interface. In [25], the authors proposed a new scheme called Distributed, Agent-based Secure Mechanism for IoD and Smart grid sensors monitoring (DASMIS). This strategy was designed to run over the hybrid peer-to-peer and client-server networks. It reduced the protocol overheads for effective operations and data communication. In this method, every node is loaded and has an initial state with a python-based agent for detecting and scanning the burned in read-only node-IDs, node MAC address, Node IP Address, system calls made, all running system programs and applications, and modifications. It also performs the data hashing and encryption and reports the changes to other peer nodes to the server in the C&C center. The agent authenticates the nodes; this is used to encipher the data communication and authorize the inter-node access. It also detects and prevents the security attacks such as DoS attacks, modification, and masquerading. In [26], the authors focused on the DRF analysis, validation, and/or data optimization to trace evidence recovery. The authors showed that the target fiber retrieval context is helpful for the investigation of the self-adhesive tapes. The authors in [27] conducted digital forensic investigations to tackle the drone incident response by using it for digital forensic analysis processes. The authors provided a detailed Drone Forensic and Incident Response Plan (DRFIR). The Federal Aviation Administration

(FAA) findings should update the requirements of its Unmanned Aerial Systems (UAS) based on two classifications of UAS. They also discussed the lack of incident responses for forensic analysis. In [28], an electromagnetic watermarking concept is used as a method for UAVs and forensic tracking. In [29], the UAVs accident investigation was done for DRF, and a forensic framework was examined. The chi-square was used for data analyses, and the independence and any considerable connection between the created groups were tested. In [30], the authors investigated drone attacks to identify security attacks for future risks. The results are based on two main factors: targets and the direction of the attacks. There may be more than one target. The main targets are GPS, embedded software, optical, audio, radar, infra-red, electromagnetic, or any cognitive channel (cognitive scrambling and stealthy communication). The attacks are made from the ground or maybe from the air. In [31], the authors classified the network traffic where drones traffic is detected by using widespread OS of ArduCopter (e.g., several DJI and Hobby king vehicles). The proposed solution can discriminate against the drones' state, either moving or steady. In [32], the authors evaluated the security susceptibility of two drones, namely Eachine E010 and Parrot Mambo FPV. The drones are vulnerable to Radio Frequency (RF) replay and custom-made controller attacks.

3. Research Methodology

The design science research methodology is adapted to drive this study [33]. It consists of two stages, as shown in Figure 2. The first stage highlights the main gaps and limitations of the DRF domain. The output of the first stage is used as input for the second stage. The second stage is used to develop the drone forensic metamodel, which is the main aim of this study. The metamodeling approach is a kind of design science method used in well-known benchmarked systems [34,35]. In the current study, this method is used to develop DRFM. The complete research methodology is presented in Figure 2.

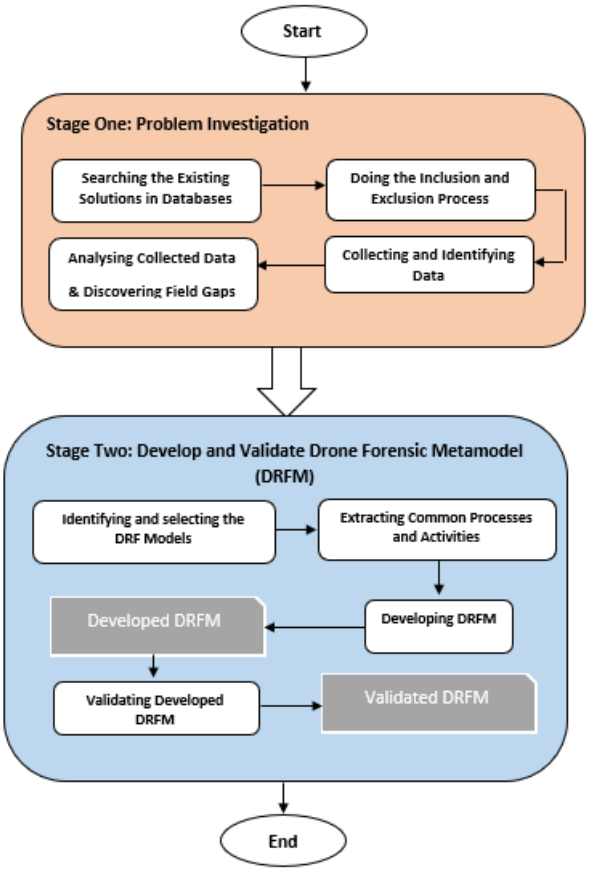

Figure 2. Research methodology framework.

3.1. Stage 1: Problem Investigation

This stage aims to highlight the main challenges and issues of the DRF domain. It consists of five steps:

(1) Searching the Existing Solutions in Databases: At this step, the existing solutions are searched in five well-known databases: IEEE Explorer, Web of Science, Springer, Scopus, and Google Scholar. The search is based on keywords like drone forensics and UAV;

(2) Doing the Inclusion and Exclusion Process: This step excludes the searched solutions. The searched protocols are identified based on the research questions presented below:

- What are the existing models of the DRF?
- What are the current limitations, challenges, advantages, and disadvantages of the DRF domain?
- Is there a generic model for the DRF domain?

(3) Collecting and Identifying Data: in this step, the authors collected data based on steps 1 and 2. The collected Data is refined based on year of publication, relevancy, and quality. Furthermore, only the papers that develop a framework, a model, or a procedure for conducting a forensic investigation on UAVs are selected. A further manual filtration approach is used where the title and name of the authors are considered to avoid duplications from multiple sources. Finally, based on the criteria mentioned above, 32 out of 102 first-selected articles were identified to be used in this study;

(4) Analyzing Collected Data and Discovering Field Gaps: After a detailed review, it is clear that the DRF domain suffers from several challenges and issues, as discussed below:

- Challenges to the Investigation Process: DRF mainly has six investigation processes, and the challenge is to select the best one to have complete harmony with the drone actions. In general, vast volumes of data are produced by a drone device, which may consist of significant evidence; this affects the whole investigation process. It is not an easy task to identify the exact device involved in the crime. It also takes more time to identify the devices engaged in crimes;
- Lack of Log Standardization: Several investigation resources have the potential to aid the investigators in clearly understanding the complete action in the device; these resources include process logs, network logs, and application logs from various resources. However, the literature has not yet offered a clear standard for logging resources through different systems;
- The Volatility of Evidence The issues related to evidence volatility in drones are much more challenging than the conventional computing platforms. This is mainly because of the low memory of sensor devices.
- Proving Ownership: Sometimes, even if digital investigators seize a crime-involved drone, they cannot physically tie it to its owner. As the owner can deny the ownership, the investigators have to prove it forensically. This poses another challenge to the investigation process, which needs to be well addressed. The following question should be answered clearly: What digital forensic approach could an investigator take to identify a drone's owner? To this end, first, the way the drone is manufactured (whether it records the information of the ground control station device or not) needs to be identified. In some cases, though, the ground control station records the drone's information. Some manufacturers have no access to this feature since no mobile application could be utilized to control the drone, and everything is limited to the drone's remote controller. Due to the high significance of the capability of proving the drones' ownership, one of the hearings in the House of Lords in the UK is dedicated to discussing this subject [36];
- The Difficulty of Supporting the Newer Drone Devices: The currently used digital forensic techniques/tools fail to support the newer drone devices fully. This has

led to many problems for digital investigators when there is a need to obtain data from such devices;

- The Absence of Strict Security Procedures: This domain still suffers from the deficiency of high-security procedures and policies, which has led to several drawbacks resulting, in turn, in cyber-incidents through the devices.
- Data Acquisition: A critical step in the digital forensics' domain is to obtain the data in a completely safe mode and then determine the acceptability of the received data in a court of law. Based on the guidelines released by the National Institute of Standards and Technology (NIST), capturing data needs to be completely repeatable and authentic and preserve the integrity of the data. On the other hand, sometimes, the way a device has been built is a barrier to this objective. Drones are of several types; each device is different in how it can be connected. Some drones may need just a USB cable, while some others might connect through specific protocols such as FTP or Telnet. In addition, different brands of drones are different in the permissions granted when accessing the drone; in most cases, access is limited to only the media folder or the system files. In other words, any consistent means do not exist currently to conduct the acquisition process on drones; for this reason, each drone might need to be moved differently. To address such challenges and obtain more knowledge of drone forensics, we need to use innovative technologies together with the knowledge obtained from these studies as starting points toward deeper insights into drone infrastructures.
- The diversity of Devices, Operation Systems, and Infrastructures: Drones are devices that run with Operation Systems (OSs) and infrastructures, making drone forensic investigation more complex. Attackers also use such characteristics in their destructive activities.
- Flight Data: Drones are devices that run with Operation Systems (OSs) and infrastructures, making drone forensic investigation more complex. Attackers also use such characteristics in their destructive activities; Flight Data: The flight data need to be recovered to identify a seized drone's flight path or determine whether the drone has entered a restricted area. The reconstruction of the drone's flight path could help this objective, but the problem is that different drones are using other methods to record the flight data, and some may not record such data at all. In some cases, the investigators may even encounter a drone with encrypted flight data. In these cases, not a single person but the technical team members who have the encrypting keys can access the flight data. Criminals usually use anti-forensic techniques such as encryption to prevent digital investigators from gaining access to their data. It should be noted that the more critical challenge here is not finding a way to access the encrypted data. Instead, it is finding the best way to deal with those drones that cannot record flight data. According to the authors in [37], changing the scope of information processing at independent locations makes it more difficult to uphold integrity, confidentiality, and accessibility, whereas carrying out an investigation could be applied to drones.
- Media Taken by the Drone: To approve or reject the violation of the law by a drone, it is important to consider its flight path and the photos and videos taken by the drone to check whether or not it has violated others' privacy. Such violation of privacy has been properly documented across the world. For instance, in Kentucky, the United States, a man shot a drone with a shotgun since the drone was flying above his house, and he decided to shoot it to protect his privacy [38]. The claim was accepted in the court of law, and the man was dismissed from all charges [37]. In [39], the authors discussed an incident in Sydney, Australia, where a drone was flying around the beach and taking photos of people, and the drone operator was unknown [39]. In addition, as a predictor of a privacy violation, the media content recorded by the drone can provide a clue as to the

drone's owner since the photos consist of some EXIF data storing the image location. The EXIF data can help forensic investigators to reconstruct the flight path from the flight data through the reconstruction of the metadata stored in the photos.

3.2. Stage 2: Develop and Validate Drone Forensic Metamodel (DRFM)

In the following, the main three steps taken to develop DRFM are explained:

1. Identifying and selecting the DRF Models: The models identified and selected at this step are based on coverage, as discussed in [40,41]. The vast convergence of concepts and terminologies is broadly applicable to fulfilling the requirements of the investigation process in DRF. The coverage metrics indicated the sourced model applicability. If the model wants to cover all DRF perspectives (i.e., technology perspective and investigation process perspective), the model should have high coverage. The model has a reduced amount of coverage value if the model only describes a specific DRF perspective, such as the technology perspective. Therefore, models (tools, methods, and algorithms) cover at least two DRF processes, i.e., investigation and technologies. These factors were identified to develop DRFM. However, the existing systems only cover the specific DRF with only one or two perspectives and are set for validation purposes;
2. Extracting Common Processes and Activities: The DRF investigation processes and activities were derived from the models selected in Step 1. Certain criteria [35,41] were followed for the investigation processes during the extraction. The criteria used to determine the DRF investigation processes and activities are as follows:
    - Extracting the investigation process from the main model design and its phases;
    - The investigation process should be based on actions to extract the main objectives, purpose, and process;
    - Avoiding any irrelevant material which is not related to DRF investigation processes;
    - Select the clear and implicit investigation processes used in existing models.
    - The above-discussed criteria and the processes were adopted to design the proposed DRFM.
3. Developing Drone Forensic Metamodel

The extracted DRF investigation activities and processes were used to build the DRFM. All the extracted activities and processes were combined and grouped. The first group examined the processes that dealt with investigation preparation, incident identification, and verification. The second group was based on data acquisition and preservation processes. The third group was focused on drone examination, reconstruction, artifact analysis, and overall forensic analysis. All the extracted DRF investigation processes were organized and merged for DRFM design. Three forensic investigation stages have been highlighted, as shown in Figure 3, where every stage has activities and processes. All stages are discussed as follows.

Stage 1: Identification Stage

Incident response management means the actions performed after any incident related to security by using technologies, infrastructure, and procedures [1]. An incident is an attack or security breach from the attacker side or any Denial of Services (DoS) attack on the network. The incident management has the following technical issues:

The Incident Response:

This stage in DRFM is used to respond to drone incidents. A typical set of components in a drone system should identify when the drone is under attack from any devices like a system, laptop, mobile phone, router, radio controller, or other components [42,43]. These all devices or components have digital evidence related to drone investigation. For components examination, more time is required. The drones should have more capabilities and flexible payloads to handle this situation. These components should be seized by the first responder, which includes including:

- Seize the Drone: In this activity, the first responder needs to search and seize the drone device, take a photo, and document it;
- Seize Radio Controller: The radio controller should be seized for examination during the DRF investigation. Although, this component is less important because it has the configuration settings that are stored and can contribute to understanding the scenario of the drone and its operation;
- Seize Mobile or Laptop: The mobile or laptop is used to manage and handle the drone device, which should be seized and moved to the lab.
- Seize Flight Record: The mobile or laptop is used to manage and handle the drone device, which should be seized and moved to the lab;
- Seize Battery and the Wi-Fi: The battery and Wi-Fi components and range are valuable in the DRF investigation. The battery is used to run the drone, whereas the Wi-Fi range extender provides a communication range to the drone. The battery stores the digital artifacts; thus, it is useful to extract the battery information [43];
- Label the Seized Data: The seized data should be marked and sent to the lab;
- Report Activities in the Identification Stage: Documenting and reporting are fundamental steps in the identification stage.

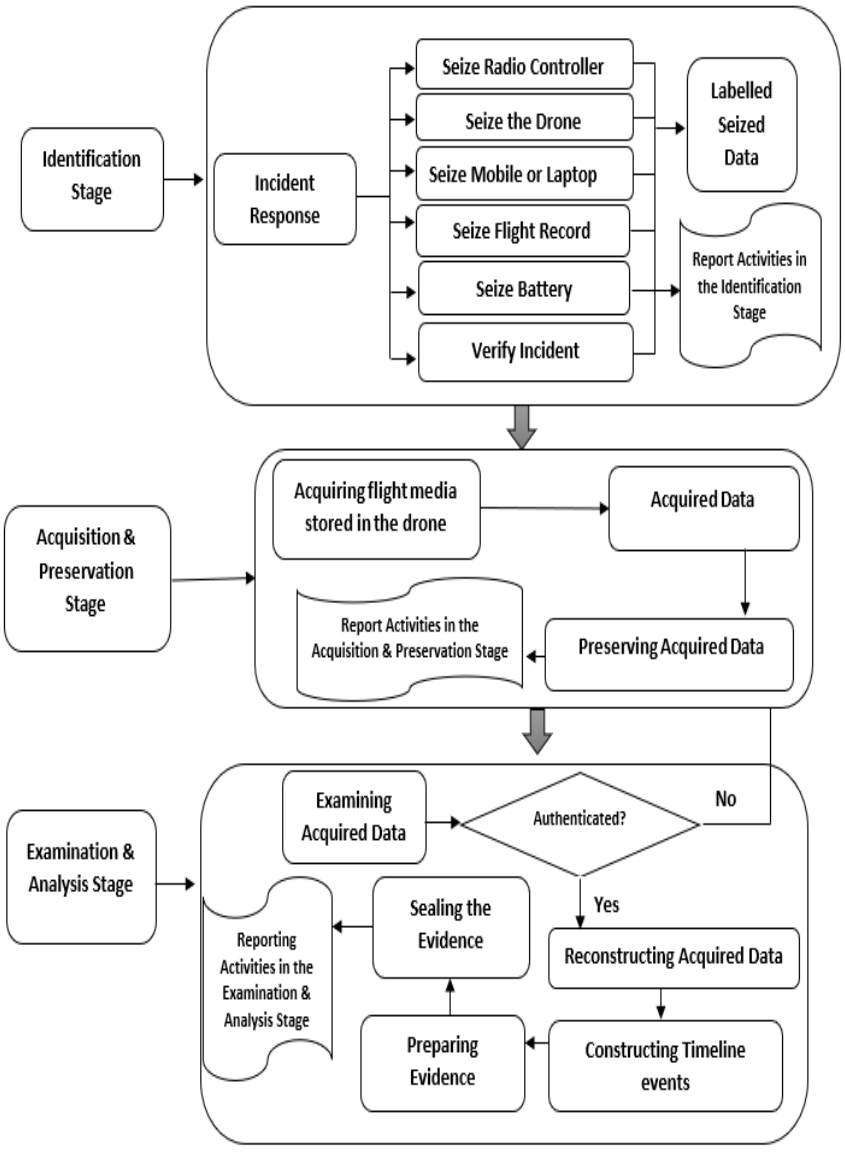

Figure 3. Drone Forensic Metamodel (DRFM).

Stage 2: Acquisition and Preservation Stage

This is the second stage of the DRFM. It is used to acquire and preserve real-time data from the seized resources identified in the identification stage. It consists of four processes, which are explained as follow:

- Acquiring Flight Media Stored in the Drone: In this process, the investigator uses some trusted mobile tools to acquire the flight media stored in the drone, for example, by using the DJI GO app [44], where the mobile device is attached with the drone and connected with remote control for flight data storage. The micro-SD card is used to store the data, which is installed under the hood of the drone. The DJI GO application is used to connect the drone with a computer for data removal and storage processes;
- Acquired Data: It is the data acquired from the drone. It includes photos, videos, and GPS paths.
- Preserving the Acquired Data: The acquired data must be preserved to protect its data integrity. The investigator should use a strong hash algorithm to protect the authenticity of the gathered data;
- Reporting the Acquisition and Preservation Stage: All the acquisition and preservation stages' steps, activities, and processes should be documented and reported.

Stage 3: Examination and Analysis Stage

The acquired data gathered in the previous stage should be examined and analyzed to identify and discover the evidence of the drone crime. This stage includes five processes, which are elaborated below:

- Examining the Acquired Data: The data acquired and preserved in the previous stage should be examined to check and verify the authenticity of the data [42]. Examiner should rehash the hashed value of the received data and check the consistency of the data. If the data is changed or modified, the examiner should return to the previous stage and collect another original copy. However, if the information is correct and has no tamper, the examiner should proceed to the next step to reconstruct the acquired data;
- Reconstructing the Acquired Data: The data examined is reconstructed to extract the evidence explaining the causes of the crime committed;
- Constructing the Timeline Events: This task can be carried out after a valid data integrity verification. This task is used to rebuild the timeline of the UAV events and reveal the evidence of the crime. Particular emphasis is expected to be taken on this step as the accuracy of the entire investigation process hinges on the accuracy of the event timeline reconstruction. Furthermore, the logic of timeline reconstruction posits that event sequencing and correlation during an investigation are built on the integrity of the reconstructed time-of-event occurrence;
- Preparing the Evidence: In this process, the investigators must identify the evidence and provide a detailed explanation. This step answers the question of who, what, when, where, and potentially, why based on the data. Who is the criminal? What time did the crime happen? And how did the crime happen?
- Sealing the Evidence: This process is used to protect the integrity of the evidence while sending it to the court.
- Reporting the Activities in the Examination and Analysis Stage: Documenting and reporting whole activities in the examination and analysis stage.

Validating Developed Drone Forensic Metamodel

This is the fourth step of the development and validation process of the DRFM. It is used to validate the consistency and applicability of the developed DRFM through metamodel transformation. The transformation is the generation of a solution model from metamodel [45]. A transformation definition is a set of transformation rules used to transfer a solution model from a metamodel to solve a specific problem. A transformation rule describes how one or more concepts in the source metamodel can be transformed

into one or more concepts in the target model. Metamodels and models relate through model transformation [46]. The acceptance of metamodels for practical use depends on a given abstraction hierarchy [47]. Model-to-model transformation is a crucial technology for model-driven engineering and supports understanding the various functionalities of our DRFM [47].

The developed DRFM needs to be transformed into various DRF solution models interoperability. This paper follows the Meta-Object Facility (MOF) methods proposed in performing a metamodel-to-model transformation for DRFM. Model transformation in MOF can be viewed in vertical and horizontal dimensions [48]. Therefore, this study focused on validating DRFM from the vertical transformation. The tracing techniques are used for this purpose [49].

The vertical transformation presents the transformation of the model from one level to a different level of modeling abstraction. The transformation can be from an upper to a lower level (e.g., from metamodel (M2) level to model (M1 and M0) level). The process of deriving individual concepts in the models is also vertical transformation. As defined by [50], a model conforms to a metamodel when the metamodel specifies every concept used in the instantiated model, and the model uses the metamodel concepts according to the rules specified by the metamodel. Thus, two aspects refer to vertical transformation Instantiation and Conformance concepts [51]. The instantiation concept instantiates one concept from the metamodel, while the Conformance concept instantiates more than one concept to derive a concept or model object from DRFM (at M2). While both, Instantiation and Conformance are categorized as a vertical model transformation, conformance can be seen as more general use of instantiation. This process supports how one or many concept/s in DRFM (at M2) derives one or many concept/s in a model (at M1 and M0).

In most cases, concepts at M1 require the use of one or more concepts from DRFM. In this paper, the vertical transformation is performed when "the M1-DRF model and M0-DRF User Data Model are being derived from its conformant M2-DRFM". M1-DRF Model and M0-DRF User Data Model transformation from M2-DRFM explains in detail using the real scenario.

Thus, the scenario was stated by [52], which demonstrates the crash drone: "A second Airbus Zephyr high altitude pseudo-satellite (HAPS) drone, built for the UK's Ministry of Defense, has crashed in Australia while on a test flight. The 25 m-wingspan aircraft reportedly crashed after encountering turbulence, according to a local news story. It was being flown from Wyndham, a remote airstrip in a northerly part of Western Australia that lies around 442 km (275 m) southwest of Darwin. The crash was said to have happened on 28 September during routine flying. With the Zephyr being a noticeably light and fragile craft, northern Australia's predictable climate (hot, dry, sunny, generally calm winds) gives a much better chance of carrying out useful test flights without seeing the weather destroying the aircraft. Indeed, Airbus probably ought to be giving lessons to the British Army and Thales on weather conditions suitable for flying unmanned aircraft. Unfortunately for Airbus, the £4.3 m Zephyr surveillance drone encountered "clear turbulence" while climbing away from the airstrip, which caused it to tumble out of control, as reported in depth by Flight Global".

Once a drone has crashed, the most important task is to identify the drone's location. The main activity of this scenario is determining the location of the drone, which includes several activities and attributes: wind speed, drone name, location of the crash, altitude, seize radio controller, ground condition, and various other attributes. Thus, to insatiate the solution models (M1 and M0) from the M2 DRFM for this scenario, the investigator needs to recognize and identify the attributes and activities/operations from the scenario, identify relevant concepts/processes, and derive the M1 and M0 solution models.

Therefore, the M1-Identification location model is required to verify the location of the crashed drone. Three relevant concepts have been recognized and identified from

the DRFM-Identification stage based on the required attributes and activities that were illustrated in Figure 4: Incident Response, Labelled Seized Data, and Report Activities.

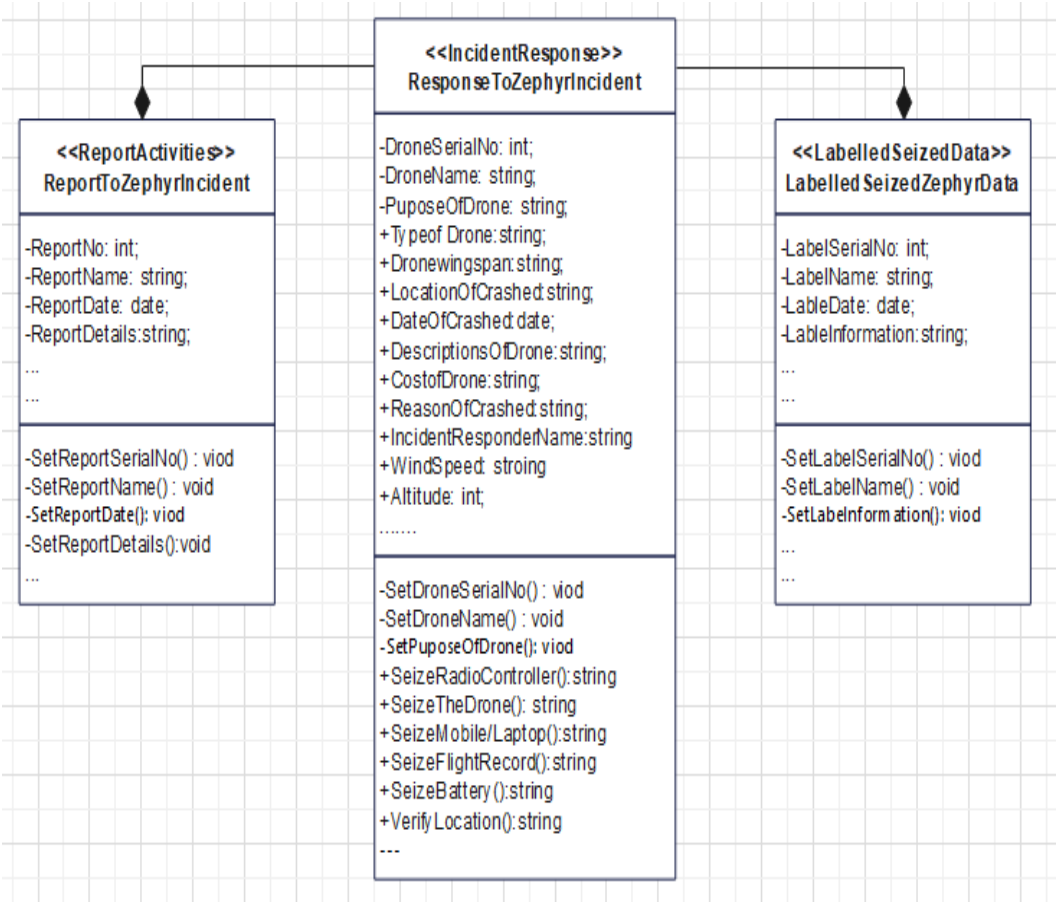

Figure 4. Instantiate M1-Identification Location Model from DRFM-Identification Stage.

The instantiated M1-Location Model conforms to DRFM, where *ResponseToZephyrIncident* instantiated from <<*IncidentResponse*>> concept, *LabelledSeizedZephyrData* instantiated from <<*LabelledSeizedData*>> concept, and *ReportToZephyrIncident* instantiated from <<*ReportActivities*>> concept.

The M1-Identification location model illustrated in Figure 4 consists of many activities instantiated from DRFM. These activities are derived from different sharing activities from other DRFM concepts and have enough information to guide domain practitioners to verify the location of the crashed drone. The guidelines offered with this derived model assist domain practitioners in instantiating several real M0-Identification Data Models easily.

Activities in the M1-Identification model form many M0-Models, as shown in Figure 4. The combined M1-Activities form several M0-Identification data models. For example, instantiate M0-SeizeRadioController model, M0-SeizeTheDrone model, M0-SeizeMobile/Laptop model, M0-SeizeFlightRecord model, M0-SizeBattery model, and M0-VerifyLocation model from M1-Identification location model. Figure 5 displays several M0-models which instantiated from the M1-Identification location model.

As shown in the above scenario, the semantics of the concepts in DRFM and their logical consistency can cover the real semantic meaning of the real concepts scenario. For example, the M2-IncidentResponse concept can be used to represent the instance of the M1-ResponseToZephyrIncident concept. Further, the M2-LabelledSeizedData concept can be used as the M1-LabelledSeizedZephyrDataconcept, while wind speed, drone name, location of the crash, altitude, seized radio controller, ground condition, and various other

attributes can be covered by the M2-IncidentResponse concept attributes and activities. The reusability of the DRF domain knowledge is one of the contributions of this study, as stated in Section 1. Thus, DRM allows domain forensic practitioners to reuse existing knowledge and produce a new DRF model to resolve their problems. The experiences support the DRF domain knowledge, stored as a Metamodel (attributes and operations), as shown in Figure 5. These reusable knowledge units can be mixed, updated, and matched as the DRF domain demands. Therefore, the M1-Models and M0-User Data Models that were used in the scenario may be reused by domain forensic practitioners to guide them to solve similar problems.

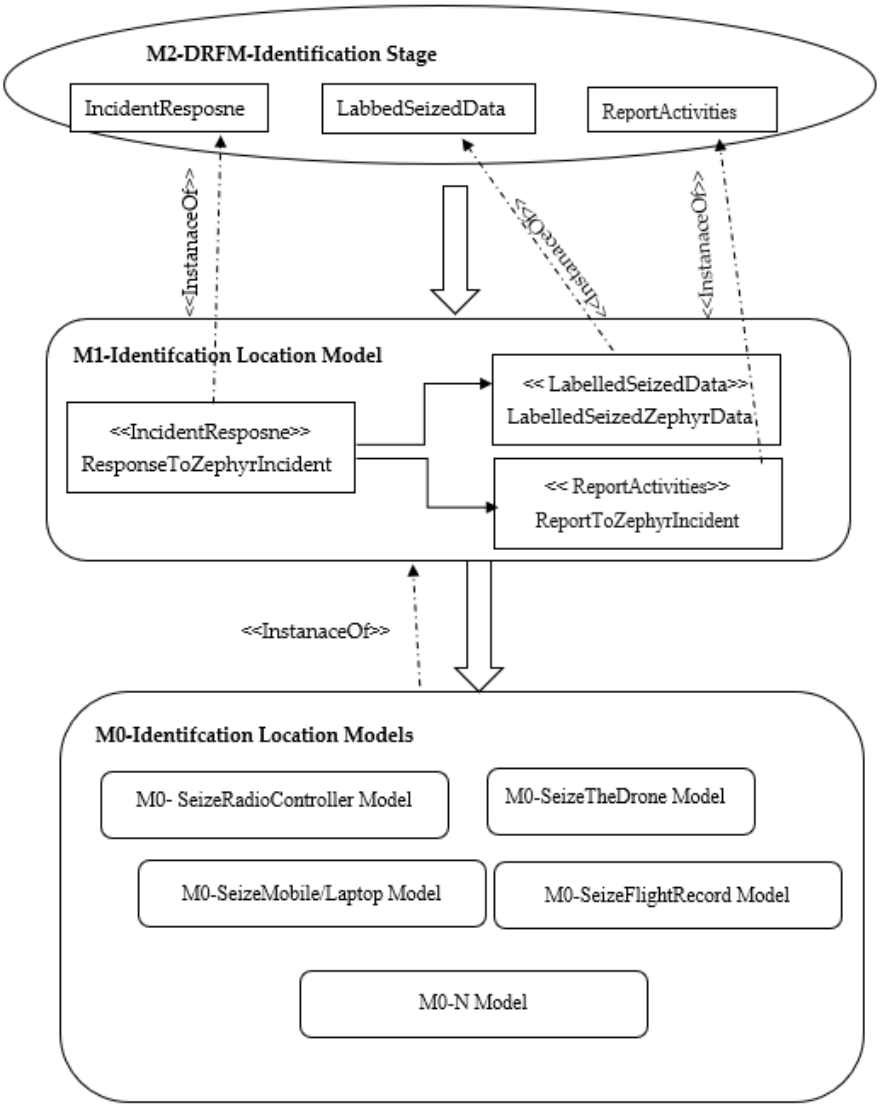

Figure 5. Several Instantized M0-Models from M1-Identification Location Model.

4. Finding and Discussion

This study highlighted the challenges and issues of the DRF domain and proposed a metamodel applicable to this domain. The main drawback of this domain is the variety of the drones' infrastructures, redundant investigation models, frameworks, processes, concepts, attributes, and tasks, making the DRF domain complex and heterogeneous. The metamodeling approach is helpful in modeling heterogeneous, complex, and ambiguous environments/domains to produce metamodeling language(metamodel). Metamodel facilitates the management, sharing, and reuse of such domain knowledge. Therefore, research in this area is significant since it discusses the importance of the metamodeling

approach in the DRF domain. The proposed DRFM can solve drone incidents by developing specific solution models from the proposed DRFM, as shown in the previous scenario.

Furthermore, it will be used by domain forensic practitioners as a guideline. The findings of this study are significant and helpful to understanding better the processes involved in the DRF domain. It contains the main concepts and processes of the DRF domain in a single model; therefore, it can facilitate fast understanding among domain forensic practitioners. Indeed, it is beneficial to the digital forensic laboratory. Also, this model is helpful for domain forensic practitioners (incident responders, examiners, investigators, and analyzers) to explain the concepts of the DRF to newly employed staff and the investigation team.

The consistency, tracing, and instantiation of the concepts of the DRFM have been validated through instantiate-specific solution models from the DRFM. One scenario has been used for this purpose. The tracing technique that has been used generally leads to thinking about and capturing the vertical relations within a DRFM and ensuring DRFM users can understand the relationships that exist within and across the DRFM.

Compared to the existing DRF works discussed in this study, the proposed DRFM model is a novel work that combines all DRF models, processes, activities, and tasks. This DRFM consists of three main levels: M2-Metamodel Level (DRFM), M1-DRF Model Level, and M0-DRF User Data Model Level. Each layer represents/governs the lower layer, as shown in Figure 6. For example, M2 represents the metamodel (meta-meta data), M1 represents the user model (metadata), and M0 represents the user data model (data). Therefore, domain practitioners can instantiate/derive their solution models from the metamodel. The benefits of the proposed DRFM are as follow:

1. The model provides communication among drones through a common layer that employs all tasks, concepts, activities, and processes for DRF;
2. It provides a conceptual roadmap to design an effective model to manage, reuse, and share DRF knowledge and information;
3. It is easily applicable, especially for DRF practitioners, to design and create new solutions by using all the attributes and operations based on the model requirements;
4. It provides quick access to DRF knowledge and helps to design new solutions.

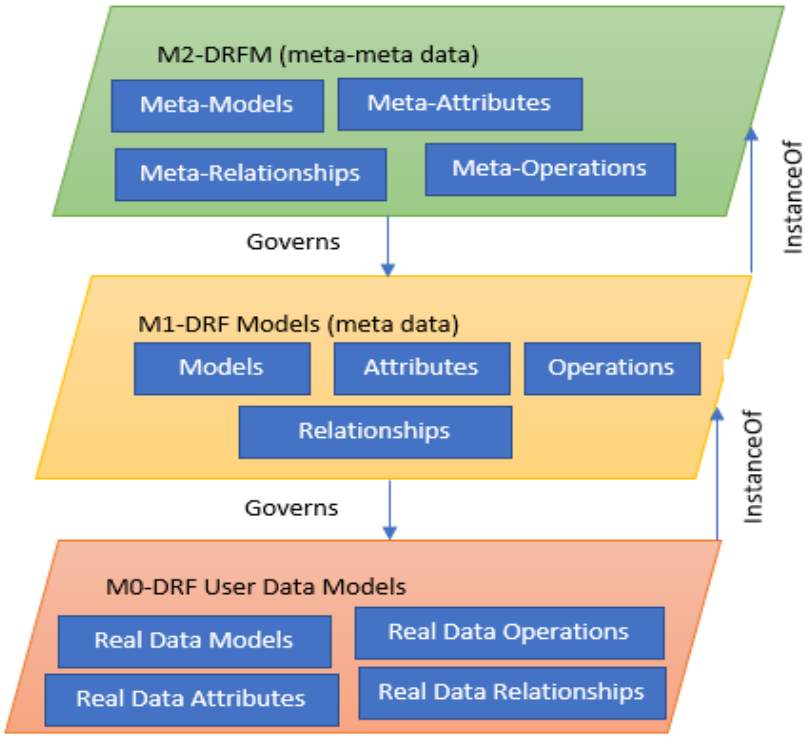

Figure 6. DRFM Levels.

5. Conclusions

The DRF domain attempts to capture and analyze drone-related incidents. Several efforts have been made to develop this domain of study: however, the fundamental research in this domain deals with drones from a technical perspective. The literature lacks a conceptual framework that organizes, structures, and facilitates the DRF domain for forensic investigation. Thus, the focus of this paper is to highlight the existing challenges and issues of the DRF domain and propose a drone forensic metamodel. The results showed that the DRF domain suffers from many problems that make it a complex, ambiguous, and heterogeneous domain for forensic practitioners and experts. To address such issues, this paper proposed DRFM to solve the heterogeneity and interoperability issues of the DRF domain. It consists of three main stages: identification stage, acquisition and preservation stage, and examination and analysis stage. The conceptual framework extracted the main challenges and suggested the solution to tackle the existing challenges and issues in DRF. Future work could focus on developing a repository for the proposed DRFM to store all relevant knowledge of the DRF domain and validate the effectiveness, completeness, and logicalness of the proposed DRFM from the horizontal transformation.

Author Contributions: Conceptualization, A.A.-D., W.M.S.Y., A.-H.M.E. and S.B.A.R.; methodology, A.A.-D. and D.S.K.; software, A.A.-D.; validation, A.A.-D., W.M.S.Y., A.-H.M.E., D.S.K. and A.A.A.; formal analysis, A.A.-D. and W.M.S.Y.; investigation, A.A.-D. and A.-H.M.E.; resources, A.A.-D. and W.M.S.Y.; data curation, A.A.-D. and A.-H.M.E.; writing—original draft preparation, A.A.-D., W.M.S.Y., A.-H.M.E., D.S.K. and A.A.A.; writing—review and editing, A.A.-D., W.M.S.Y., A.-H.M.E., D.S.K. and A.A.A.; visualization, A.A.-D., W.M.S.Y. and A.-H.M.E.; supervision, A.A.-D., W.M.S.Y., S.B.A.R. and A.-H.M.E.; project administration, A.A.-D., S.B.A.R. and W.M.S.Y.; funding acquisition, D.S.K. and A.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This project is funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R308), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement: Not applicable.

Acknowledgments: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R308), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kovar, D.; Dominguez, G.; Murphy, C. UAV (aka drone) Forensics. In Proceedings of the SANS DFIR Summit, Online, 9 October 2016; pp. 23–24.
2. Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Razak, S.; Ghabban, F.M. Research Challenges and Opportunities in Drone Forensics Models. *Electronics* **2021**, *10*, 1519. [CrossRef]
3. Abdullah, A.; Othman, S.H.; Razali, M.N. Structuring knowledge on house Price Volatility through a metamodel. *ARPN J. Eng. Appl. Sci.* **2015**, *10*, 17785–17795.
4. Colette, R. Modeling the Requirements Engineering Process. In Proceedings of the 3rd European-Japanese Seminar on Information Modelling and Knowledge Bases, Budapest, Hungary, 31 May–3 June 1993.
5. Mhatre, V.; Chavan, S.; Samuel, A.; Patil, A.; Chittimilla, A.; Kumar, N. Embedded video processing and data acquisition for unmanned aerial vehicle. In Proceedings of the 2015 International Conference on Computers, Communications, and Systems (ICCCS), Kanyakumari, India, 2–3 November 2015; pp. 141–145.
6. Roder, A.; Choo, K.-K.R.; Le-Khac, N.-A. Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study. *arXiv* **2018**, arXiv:1804.08649. [CrossRef]
7. Horsman, G. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digit. Investig.* **2016**, *16*, 1–11. [CrossRef]
8. Ikuesan, R.A.; Ganiyu, S.O.; Majigi, M.U.; Opaluwa, Y.D.; Venter, H.S. Practical Approach to Urban Crime Prevention in Developing Nations. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security, Marrakech, Morocco, 31 March–2 April 2020; pp. 1–8.
9. Maarse, M.; Sangers, L.; van Ginkel, J.; Pouw, M. *Digital Forensics on a DJI Phantom 2 Vision+ UAV*; University of Amsterdam: Amsterdam, The Netherlands, 2016; Volume 1, p. 22.
10. Procházka, T. Capturing, Visualizing, and Analyzing Data from Drones. Bachelor's Thesis, Charles University, Prague, Czech Republic, 2016.
11. Mohan, M. Cybersecurity in Drones. Ph.D. Thesis, Utica College, Utica, NY, USA, 2016.

12. Jain, U.; Rogers, M.; Matson, E.T. Drone forensic framework: Sensor and data identification and verification. In Proceedings of the SAS 2017—2017 IEEE Sensors Applications Symposium, Glassboro, NJ, USA, 13–15 March 2017; pp. 1–6. [CrossRef]
13. Clark, D.R.; Meffert, C.; Baggili, I.; Breitinger, F. DROP (DRone open source parser) your drone: Forensic analysis of the DJI phantom III. *Digit. Investig.* **2017**, *22*, S3–S14. [CrossRef]
14. Prastya, S.E.; Riadi, I.; Luthfi, A. Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence. *Int. J. Comput. Sci. Inf. Secur.* **2017**, *15*, 280–285.
15. Bucknell, A.; Bassindale, T. An investigation into the effect of surveillance drones on textile evidence at crime scenes. *Sci. Justice* **2017**, *57*, 373–375. [CrossRef]
16. Llewellyn, M. *DJI Phantom 3-Drone Forensic Data Exploration*; Edith Cowan University: Perth, Australia, 2017.
17. Barton, T.E.A.; Azhar, M.A.H. Bin Forensic analysis of popular UAV systems. In Proceedings of the 2017 7th International Conference on Emerging Security Technologies (EST), Canterbury, UK, 6–8 September 2017; pp. 91–96. [CrossRef]
18. Kebande, V.R.; Venter, H.S. Adding event reconstruction to a Cloud Forensic Readiness model. In Proceedings of the 2015 Information Security for South Africa (ISSA), Johannesburg, South Africa, 12–13 August 2015; pp. 1–9.
19. Bouafif, H.; Kamoun, F.; Iqbal, F.; Marrington, A. Drone Forensics: Challenges and New Insights. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–6. [CrossRef]
20. Esteves, J.L.; Cottais, E.; Kasmi, C. Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV. In Proceedings of the 2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE), Amsterdam, The Netherlands, 7–30 August 2018; pp. 48–52.
21. Gülataş, İ.; Baktır, S. Unmanned aerial vehicle digital forensic investigation framework. *J. Nav. Sci. Eng.* **2018**, *14*, 32–53.
22. Dawam, E.S.; Feng, X.; Li, D. Autonomous arial vehicles in smart cities: Potential cyber-physical threats. In Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 28–30 June 2018; pp. 1497–1505.
23. Renduchintala, A.; Jahan, F.; Khanna, R.; Javaid, A.Y. A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. *Digit. Investig.* **2019**, *30*, 52–72. [CrossRef]
24. Renduchintala, A.L.P.S.; Albehadili, A.; Javaid, A.Y. Drone Forensics: Digital Flight Log Examination Framework for Micro Drones. In Proceedings of the International Conference Computational Science Computational Intelligence CSCI 2017, Las Vegas, NV, USA, 14–16 December 2017; pp. 91–96.
25. Fitwi, A.; Chen, Y.; Zhou, N. An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring. In Proceedings of the Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII, Baltimore, MD, USA, 14–18 April 2019; p. 19. [CrossRef]
26. Jones, Z.V.; Gwinnett, C.; Jackson, A.R.W. The effect of tape type, taping method and tape storage temperature on the retrieval rate of fibres from various surfaces: An example of data generation and analysis to facilitate trace evidence recovery validation and optimisation. *Sci. Justice* **2019**, *59*, 268–291. [CrossRef]
27. Salamh, F.E.; Rogers, M. Drone Disrupted Denial of Service Attack (3DOS): Towards an Incident Response and Forensic Analysis of Remotely Piloted Aerial Systems (RPASs). In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 704–710.
28. Esteves, J.L. Electromagnetic Watermarking: Exploiting IEMI effects for forensic tracking of UAVs. In Proceedings of the EMC EUROPE—2019 International Symposium on Electromagnetic Compatibility, Barcelona, Spain, 2–6 September 2019; pp. 1144–1149. [CrossRef]
29. Mei, N. Unmanned Aircraft Systems Forensics Framework an Approach to Unmanned Aircraft Systems Forensics Framework. Ph.D. Thesis, Capitol Technology University, Laurel, MD, USA, 2019.
30. Le Roy, F.; Roland, C.; Le Jeune, D.; Diguet, J.P. Risk assessment of SDR-based attacks with UAVs. In Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland, 27–30 August 2019; pp. 222–226. [CrossRef]
31. Sciancalepore, S.; Ibrahim, O.A.; Oligeri, G.; Di Pietro, R. Detecting drones status via encrypted traffic analysis. In Proceedings of the WiseML 2019—ACM Workshop on Wireless Security and Machine Learning, Miami, FL, USA, 15–17 May 2019; pp. 67–72. [CrossRef]
32. Lakew Yihunie, F.; Singh, A.K.; Bhatia, S. Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles. *Smart Innov. Syst. Technol.* **2020**, *141*, 701–710.
33. March, S.T.; Smith, G.F. Design and natural science research on information technology. *Decis. Support Syst.* **1995**, *15*, 251–266. [CrossRef]
34. Al-Dhaqm, A.; Razak, S.; Othman, S.H.; Ngadi, A.; Ahmed, M.N.; Mohammed, A.A. Development and validation of a database forensic metamodel (DBFM). *PLoS ONE* **2017**, *12*, e0170793. [CrossRef] [PubMed]
35. Al-Dhaqm, A.; Razak, S.; Othman, S.H.; Choo, K.-K.R.; Glisson, W.B.; Ali, A.; Abrar, M. CDBFIP: Common database forensic investigation processes for Internet of Things. *IEEE Access* **2017**, *5*, 24401–24416. [CrossRef]
36. Kerner, M.; Berry, M.; Zammit, B.; Chongolnee, B. *Drones vs. Privacy in The Modern Era*; Benya Chongolnee: San Diego, CA, USA, 2017.
37. Matyszczyk, C. *Judge Rules Man Had Right to Shoot Down Drone over His House*; CNET: San Francisco, CA, USA, 2015; Volume 28.
38. Frank, M. *Drone Privacy: Is Anyone in Charge*; Consumer Reports; Available online: https://www.consumerreports.org/electronics/drone-privacy-is-anyone-in-charge-a1127325389/ (accessed on 11 February 2016).
39. Gair, K. *Privacy Concerns Mount as Drones Take to the Skies*; CNET: San Francisco, CA, USA, 2015; Volume 12.

40. Caro, M.F.; Josyula, D.P.; Cox, M.T.; Jiménez, J.A. Design and validation of a metamodel for metacognition support in artificial intelligent systems. *Biol. Inspired Cogn. Archit.* **2014**, *9*, 82–104. [CrossRef]
41. Ali, A.; Abd Razak, S.; Othman, S.H.; Mohammed, A.; Saeed, F. A metamodel for mobile forensics investigation domain. *PLoS ONE* **2017**, *12*, e0176223. [CrossRef]
42. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D. A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Comput. Intell. Neurosci.* **2022**, *2022*, 8002963. [CrossRef]
43. Al-Room, K.; Iqbal, F.; Baker, T.; Shah, B.; Yankson, B.; MacDermott, A.; Hung, P.C.K. Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models. *Int. J. Digit. Crime Forensics* **2021**, *13*, 1–25. [CrossRef]
44. Cabassi, J.; Lazzaroni, M.; Giannini, L.; Mariottini, D.; Nisi, B.; Rappuoli, D.; Vaselli, O. Continuous and near real-time measurements of gaseous elemental mercury (GEM) from an Unmanned Aerial Vehicle: A new approach to investigate the 3D distribution of GEM in the lower atmosphere. *Chemosphere* **2022**, *288*, 132547. [CrossRef]
45. Mens, T.; Van Gorp, P. A taxonomy of model transformation. *Electron. Notes Theor. Comput. Sci.* **2006**, *152*, 125–142. [CrossRef]
46. Štuikys, V.; Damaševičius, R. A model-driven view to meta-program development process. In *Meta-Programming and Model-Driven Meta-Program Development*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 127–142.
47. Gardner, T.; Griffin, C.; Koehler, J.; Hauser, R. A review of OMG MOF 2.0 Query/Views/Transformations Submissions and Recommendations towards the final Standard. In *MetaModelling for MDA Workshop*; Citeseer: Princeton, NJ, USA, 2003; Volume 13, p. 41.
48. France, R.; Bieman, J.M. Multi-view software evolution: A UML-based framework for evolving object-oriented software. In Proceedings of the IEEE International Conference on Software Maintenance, ICSM 2001, Florence, Italy, 7–9 November 2001; pp. 386–395.
49. Sargent, R.G. Model verification and validation. In *Modeling and Simulation in the Systems Engineering Life Cycle*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 57–65.
50. Rose, L.M.; Kolovos, D.S.; Paige, R.F.; Polack, F.A.C. Model migration with epsilon flock. In Proceedings of the International Conference on Theory and Practice of Model Transformations, Málaga, Spain, 28 June–2 July 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 184–198.
51. Henderson-Sellers, B. Bridging metamodels and ontologies in software engineering. *J. Syst. Softw.* **2011**, *84*, 301–313. [CrossRef]
52. Corfield, G. Second MoD Airbus Zephyr Spy Drone Crashes on Aussie Test Flight. 2019. Available online: https://www.theregister.com (accessed on 11 October 2019).