electronics

Review

Research Challenges and Opportunities in Drone Forensics Models

Arafat Al-Dhaqm [1,2], Richard A. Ikuesan [3], Victor R. Kebande [4,*], Shukor Razak [1] and Fahad M. Ghabban [5]

[1] School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia (UTM), Skudai 81310, Malaysia; mrarafat1@utm.my (A.A.-D.); shukorar@utm.my (S.R.)
[2] Department of Computer Science, Aden Community College, Aden 999101, Yemen
[3] Department of Cybersecurity and Networking, School of Information Technology, Community College Qatar, Doha 00974, Qatar; richard.ikuesan@ccq.edu.qa
[4] Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 971 87 Luleå, Sweden
[5] Information System Department, College of Computer Science and Engineering, Taibah University, Madina 42353, Saudi Arabia; fghaban@taibahu.edu.sa
* Correspondence: victor.kebande@ltu.se

Abstract: The emergence of unmanned aerial vehicles (also referred to as drones) has transformed the digital landscape of surveillance and supply chain logistics, especially in terrains where such was previously deemed unattainable. Moreover, the adoption of drones has further led to the proliferation of diverse drone types and drone-related criminality, which has introduced a myriad of security and forensics-related concerns. As a step towards understanding the state-of-the-art research into these challenges and potential approaches to mitigation, this study provides a detailed review of existing digital forensic models using the Design Science Research method. The outcome of this study generated in-depth knowledge of the research challenges and opportunities through which an effective investigation can be carried out on drone-related incidents. Furthermore, a potential generic investigation model has been proposed. The findings presented in this study are essentially relevant to forensic researchers and practitioners towards a guided methodology for drone-related event investigation. Ultimately, it is important to mention that this study presents a background for the development of international standardization for drone forensics.

Keywords: drone forensics; unmanned aerial vehicles (UAV); digital forensics

check for updates

Citation: 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. https://doi.org/10.3390/electronics10131519

Academic Editors: Ahmed M. Al-Samman, Tawfik Al-Hadhrami, Ahmad Al Shami and Fuad Alnajjar

Received: 8 May 2021
Accepted: 16 June 2021
Published: 23 June 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Unmanned Aerial Vehicles (UAVs)/Piloted Aircraft Systems (RPAS) or drones are small pilotless aircraft that can be controlled remotely. Even though the use of drones had been formerly confined to military purposes and those maintaining enthusiasm for aircraft, in latest years, their civilian usage has grown significantly from military to private sectors, industries and the society at large. Their increasing popularity which is partly fueled by the fact that UAVs are more reasonably priced today is also seen by their applications within a broad range of settings, ranging from commercial to government to military, and so on. In 2015, for example, Amazon revealed its plans to launch UAV delivery systems, Amazon Prime Air [1], a well-known international parcel delivery company, also reportedly performed test flights (parcelcopter) to Juist, an island in the North Sea. The prevalence of the digital lifestyle as a 'new normal' due to the current COVID-19 global pandemic has further led to the prevailing deployment of UAVs as parcelcopter. Additionally, UAVs have been explored in law enforcement settings (e.g., to patrol and police surveillance) [1,2], search and rescue missions [3], agricultural maintenance, filming, deterring and identification of poaching [1].

A recent study has proposed the deployment of UAVs that have dynamic capabilities towards the enhancement of policing capabilities in developing nations. These possibilities, though still largely unexplored, reveal the potential of drones in enhancing the living aspect of humans daily. However, with such potentials also comes the tendency for abuse. Similar to other popular commercial and consumer devices, there are diverse situations that allow drones to be misused. A solution that can help to discover how and where drone misuse is carried on is to employ scientific investigation processes. Device-level forensics [4–6], which mainly focuses on conducting forensic investigations of connected and sensor-based devices is presented as a more suitable approach that can be used to forensically investigate UAVs. This is because drones have sensing capabilities and tracking their movements may require amalgamating the two. Normally, conducting digital forensics in such devices requires one to locate data that has a possibility of being stored across different locations, for example, on the network, routers, SD cards, etc. This would, therefore, require proper incidental planning and preparation [7,8] approach to extract forensic features that can help create a forensic hypothesis.

The drone forensics (DRF) domain is a significant domain used to identify, collect, preserve, reconstruct, analyze and document potential UAV incidents. However, it is a heterogeneous, complex and ambiguous domain due to the variety and multidimensional nature of UAVs. Numerous specific DRF models and frameworks have been proposed to solve specific UAV scenarios but there is a lack of a structured and unified model to facilitate, manage, share and reusing of DRFs tasks and activities.

Thus, this paper reviews from a digital forensic perspective, the existing body of research carried out formerly in developing DRFs capability and the underlying challenges attributable to these studies. Furthermore, the paper discusses the issues that may arise in this context by leveraging the thematic composition of the reviewed studies and then proposed an integrated forensic investigation model to structure and organize the DRFs domain. Potential solutions that can be employed to effectively address these issues are further highlighted.

The rest of the paper is structured as follows: Section 2 provides a synopsis of the potential sources of digital evidence from a drone device, while Section 3 presents the research methodology adopted for this study. Findings and limitations of the existing DRFs studies are also presented in this section. Section 4 provides insight into the potential research directions for DRFs. Section 5 presents the proposed unified forensic model for UAVs, while Section 6 introduces a comparison of the proposed model with existing DRF models. Discussion and conclusion of this work are presented in Sections 7 and 8, respectively.

2. Potential Digital Forensic Artifacts Sources for Drones Forensics

Drones' device categorization can be carried out based on diverse criteria. However, given the forensic perspective of this study, the drone functionalities are explored from the evidential impact perspective. Therefore, only components wherein potential digital artifacts can be identified are discussed in this section. As asserted in [9], drone functionalities can be classified to include the Ground-station controller, (multi)rotor system, on-board Flight Control Board (FCB), Electronic Speed Controller (ESC), on-board Power Management System (PMS) as well as the Transceiver Control Unit (TCU). In terms of potential digital forensic artifacts, the Ground-station controller, FCB, ESC, PMS and the TCU present a potentially reliable source of evidence. Log and memory information can be extracted from the ground station controller unit. This could be a software platform, or a customized base-station design to interact with the FCB.

The FCB is the brain of the drone [10], as it integrates and coordinates information from every functional unit of the drone. These include the mounted sensors, the flight trajectory and navigation control, the inertial measurement and controls, power management as well as interaction with the ground station. Furthermore, the core functionality is the ESC. It is an electronic circuit house that manages the speed and overall efficiency of the drone movement. Given that a drone is unmanned, the TCU plays a very important role. It provides a medium for communication and control between the FCB and the base station.

In addition, it provides a medium of communication for the diverse sensors mounted on the drone.

Digital forensic artifacts from drone devices can take the form of data stored in the memory (a viable application of memory forensics), contents of diverse log files, as well as electromagnetic (EM) wave data. The FCB and the ESC are potential sources of memory artifacts, that can be extracted directly from the components of the FCB, ESC and PMS, respectively. These components include flight record data, flight control data, data from the mounted transceivers and sensors, as well as information from the internal monitoring unit of the drone. However, the digital artifacts (in the form of EM signals) from respective transceivers and mounted sensors could provide further corroborative information for the investigation. In this regard, the TCU can be leveraged to extract primary EM signals which can be further processed to extract secondary corroborative digital artifacts. Signal processing methodologies are often adopted to complement the process of forensic data identification and extraction. The architecture of UAVs and protocols that support its communication is shown in Figure 1.

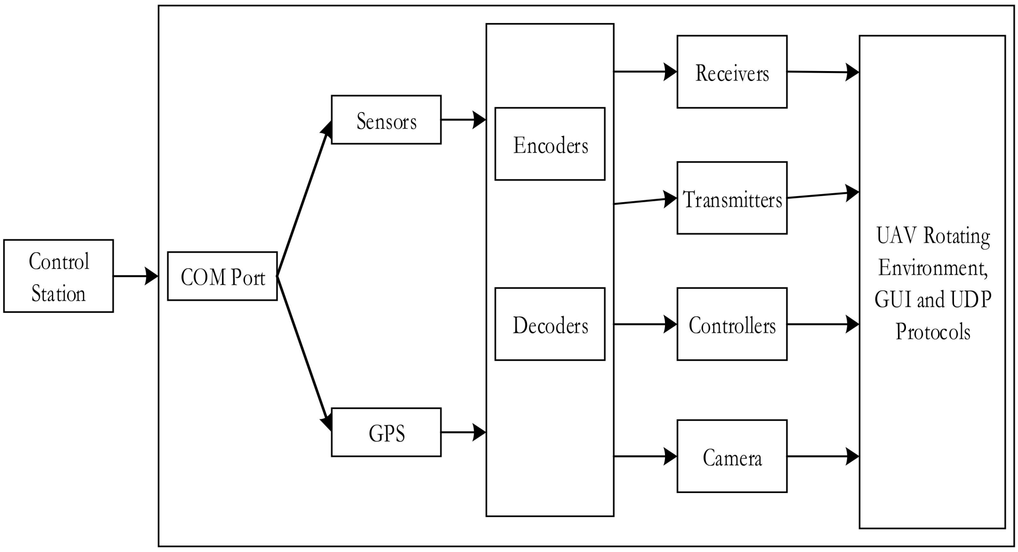

Figure 1. UAV architecture composition.

Based on the concept of the Spoonbill [11], the UAV architecture mainly can be viewed from a high-level architecture that relies mainly on a GUI that has a UDP protocol that can facilitate communication with other applications. As is shown in Figure 1, the UAV architecture consists of the following: Sensors, COM ports, Encoders, decoders, Global Positioning System (GPS), Control base station, GUI and Wireless support, receivers, transmitters, controllers and a camera. In addition, the architecture is positioned with a camera that can relay ongoing activities in real-time. Basically, the UAV protocols allows interactions by way of connections via (UDP or TCP) protocols, where the connection is initiated remotely or in real-time. In this context, the IP address of the specific UAV is registered to allow identification and attribution during data transmission for purposes of end-to-end communication.

3. Methodology

To conduct the state of the art of DRFs, a systematic review process was conceptualized. The method employed with their respective processes is further highlighted in Figure 2. This method, adapted a design science research approach, as explored in similar studies [12–14]. The topic for the present study was selected using questions concerning the main subject of the research and considering the background of the topic of focus. The following three fundamental questions outline the composition of the research:

1. What DRFs models exist currently in literature?

2. Are there any unified models/frameworks for the DRFs domain?
3. What are the limitations of the currently used DRFs models?

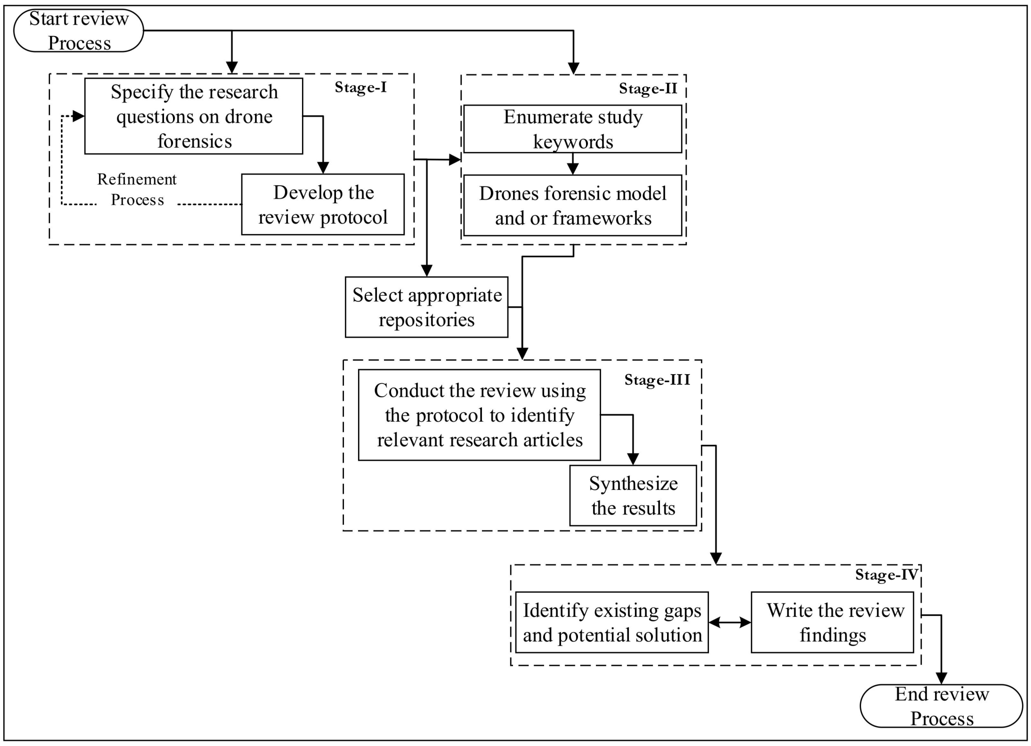
Start review Process
Stage-I
Specify the research questions on drone forensics
Develop the review protocol
Refinement Process
Stage-II
Enumerate study keywords
Drones forensic model and or frameworks
Select appropriate repositories
Stage-III
Conduct the review using the protocol to identify relevant research articles
Synthesize the results
Stage-IV
Identify existing gaps and potential solution
Write the review findings
End review Process

Figure 2. Conceptualized methodology.

To achieve the solution, this study has been explored in two distinct phases: Selection of the databases, reviewing current literature and highlighting the findings and limitations if any, these are explained next.

3.1. Phase 1: Selection of Online Databases and Finding Related Literature

To select an online database, a definite scope was defined for reviewing the literature. The term "Drone Forensics" was searched (as the searching keywords) in such a way as to collect the models proposed in the DRFs field. Furthermore, composite search phrases that integrate frameworks and models were included in the search process. To achieve this, the keywords ["Drone Forensics" + Model] and ["Drone Forensics" + Frameworks] were implemented on the selected academic repositories. This is covered in Stages I and II of the conceptual methodology presented in Figure 2. The output of Stage-1 is used to identify the appropriate repository for subsequent investigation. The appropriateness of the repository selection process involves determining the relevance of existing repositories to the extracted keywords. Based on the preliminary study conducted using the Google Scholar search engine, some repositories were observed to contain literature that is relevant to drone forensics in general. The selected repositories include Web of Science, IEEE Explore, Scopus, Springer Link, ACM, ScienceDirect. These repositories were used to search for literature that is relevant to the DFRs field. Regarding the time scope, the search space was confined to the studies published between the years 2000 and 2020. For this paper, only research articles, conference papers, dissertations, books and book chapters were considered. Furthermore, the exclusion includes articles that attempt to develop a framework, a model or a procedure for conducting a forensic investigation on UAVs. To avoid duplications from multiple sources, a further manual filtration approach using the title and name of the authors was considered. Table 1 summarizes the details of the result of the search protocols employed in this study. Finally, 32 out of 102 articles were identified to align with the topic of DRFs processes and technology.

Table 1. Systematic Review Protocols.

Database Search Engines	DRFs-Related Articles	Selected Articles
Web of Science	9	4
Scopus	17	1
IEEE Explore	3	12
Springer Links	4	3
Google Scholar	60	12
ACM	1	0
Science Direct	8	0
Total	102	32

3.2. Phase 2: Reviewing the Current Literature

A review of the literature revealed that scholars and developers have generally approached the DRFs field through various categories such as (1) forensic analysis, (2) non-forensic analysis, (3) forensic framework and (4) application in forensic analysis. A total of 29 models were found in the process of literature review as shown in Table 1, which were centered completely upon the DRFs topic. For example, [1,15] provide a discussion on the ways to recover the required evidence in case a drone is investigated under digital forensics circumstances. These studies were mainly focused upon the wireless forensic aspects, whereas that of [1] was centered upon all parts of a drone. However, both highlighted the Linux Operating System and its desirable capacities in the collection of evidence on the Linux file system. Remember that drones require an OS to work. Studies in [16,17] attempted to design a certain tool with the help of Java-FX to be well applied to the visualization of real-time flight control. This tool cannot be implemented directly in forensics; though it can establish an effective connection between the controller and the drone for data transferring procedures, and it can visualize sensor parameters such as IMU, GPS and altitude for pilots, hence providing a flight with a high level of safety.

Similarly, a study in [1] forensically analyzed 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?" In addition, a concise investigation of counter forensic methods was conducted to ascertain if the flight path record can be detected. In another research, a preliminary forensic analysis of the Parrot Bebop was accomplished by [2], where the Parrot Bebop can be named as the only UAV that is comparable with the Parrot AR Drone 2.0. From the research in [1], the author addressed the key challenges in UAV forensic analyses and then carried out his investigation on two separate parts: the UAV and flight controller. The flight-related data were retrieved from the device in the form of '.pud' files. Moreover, at each session that happened between the controller and UAV, a new .pud file was formed. At the opening point of each .pud file, a set of metadata was explored, which consisted of the serial number of the UAV, the flight date and time, the model of the flight controller and the flight controlling application. Then, an attempt was made to identify the videos/images recorded by the UAV's onboard camera. The images preserved the EXIF data that contained the latitude/longitude coordinates of the places from which the images were taken. The ownership can be established only when the UAV and controller have been seized through the identification of the device serial number. Research in [16] attempted to generally review DRFs with the use of DJI Phantom 2. They carried out breakdown analyses of the hardware and software components of the drone and discussed the ways they can be applied to the implementation of DRFs. Their findings succeeded in the establishment of a belief in the persistence and scope of DRFs. Furthermore, this research provides a proper opportunity for scrutinizing deeper into this concept and improving it. In addition, Ref. [18] worked on the integration of the visualizing data retrieved from drones and a non-forensic approach. This study was carried out on the Parrot AR Drone 2.0. With the use of their self-designed application, the log parameters from flight data were visualized although the evaluation was performed on only a small number of drones. Furthermore, study in [17] analyzed susceptibilities and uses of drones as well as their relationship with cybersecurity-related issues. The findings confirmed that in cases where drones are hacked and misused by opponents, it can lead to considerable threats or ramifications as a result. This research mainly tests the benefits of applying drones to an extensive range of situations, from using them as children's toys to applying them as weapons for mass destruction.

A forensic framework comprising 12 phases was designed by [19] to introduce a new approach through which UAVs can be investigated systematically. They conducted extensive tests on five commercial UAVs, including the Parrot AR Drone 2.0, to identify and understand the relationships among different components. In addition, an experiment was carried out for validation of the proposed framework. Each UAV involved in the testing was modified by the removal and/or addition of some of its components. It was accomplished mainly for the aim of checking whether the framework encompassed all of the different components that generally exist in any basic commercial UAV and also to test its applicability to a comprehensive UAV analysis. The authors concluded that the absence of law enforcement training processes in the field of UAV is a key issue that hinders the effective mitigation of attacks. Any of the five UAVs were not subjected to forensic analyses; though, a valuable framework was finally provided, which can help scholars to examine and analyze stages. The first wide-ranging analysis of the DJI Phantom 3 Standard was carried out by [20]. In that study, a forensically sound open-source Drone Open-Source Parser (DROP) tool was also developed. The under-investigation UAV was flown to two different sites. Afterward, the data acquired were divided into three parts: controller, drone and phone/tablet. Ultimately, two files of interest were explored: (1) the '.dat' files generated by the UAV, and (2) the '.txt' files generated by the DJI GO application. These files were decrypted and decoded; then, flight information related to Wi-Fi connections, GPS locations, flight status, remote control, motors, etc. were taken out. After the analysis of the acquired data and understanding the proprietary file structures, the DROP tool was developed to analyze the evidentiary files.

Findings from [20] showed that if a UAV is turned on, the integrity of the data kept on its internal storage can be impacted. A new .dat file was generated each time the UAV was turned on. Moreover, it was found out that in case the SD card was at or near its full capacity, turning on the UAV caused the immediate removal of the oldest data in a way not to be coverable later. As stated by [20], although their research offered an appropriate point to start UAV forensic analysis, further research is required to cover the broad range of UAVs obtainable presently. In addition, the study in [19] provides a comprehensive discussion regarding the ways the GPS coordinates can be applied as location evidence when investigating the crimes committed using drones. The above-mentioned authors attempted to extract the system logs. They also made a visualization of GPS coordinates on maps, where web-based third-party platforms were employed for the aim of plotting the flight path. In another project, a forensic model was introduced by [19] to determine and authenticate different drone components that can be employed in committing unlawful deeds. They were centered on the analysis of physical evidence gathered by investigators from the crime scene along with GPS-related data and any multimedia found on board. Their research was carried out on five commercial drones together with their components once seized at crime scenes.

A key challenge in lowering drone attacks is the shortage of law enforcement training processes in this field. A study in [20] also designed an open-source tool called Drone Open Source Parser (DROP) capable of effectively analyzing the DAT files that are extracted from the internal storage of drones. This was further compared with the .TXT file stored in the mobile controller device, which establishes a connection between user and device through correlating these data. Similarly, a study in [21] examines the impacts of a quadcopter's downwash to check whether it can affect the retention of textile evidence in crime scenes.

The authors recorded the yarn retention upon several various floors after a drone fly-past at different heights and after taking off at preset distances from the evidence area. This study was carried out to assist the police forces who aim to employ quadcopter drone surveillance in the future to uphold the integrity of the scene by adhering to or flying above any minimum "safe height" and "safe distance" determined. In another study, [22], an attempt to find out the correlation of the flight data amongst the drone, SD card and mobile phone, was explored. The establishment of a link between the drone and the suspect applies to the facilitation of criminal investigations. Native software to personal UAV devices can provide a plethora of digital artifacts from GPS timestamps and waypoints, the number of satellites connected, barometer, roll, pitch, distance, azimuth, battery status, video and photos. [23] analyzed the essential major log parameters of the autonomous drone and suggested the use of comprehensive software architecture related to DRFs with preliminary results. The authors expected their proposed software to make available a user-friendly graphical user interface (GUI) on which users would be capable of extracting and examining the onboard flight information. They expected to have a contribution to the forensic science community by proposing a tool applicable to investigations on drone-related crime cases. According to [24], open-source tools such as CsvView and ExifTool have been employed by several scholars for the aim of extracting artifacts from mobile applications of drones with the use of mobile forensic techniques. In that study, Kali (which is a Linux distribution) and Windows were employed as forensic workstations to carry out the required forensic analyses on two drones, DJI Phantom 3 and A.R Drone.

The open-source tools, e.g., Geo-Player, were applied mainly to the visualization of flight path data. Due to the nonexistence of an appropriate build environment that includes configuration tools, a package manager and a compiler in the UAV system, this option needs to extensively change the data that exist in the UAV. Therefore, it was stopped in favor of the logical level acquisition. It was achieved by mounting a forensic mass storage device onto the UAV; then, files were completely copied from the mounted "/data" partition with the use of the "cp" command. Digital forensics was also applied by [25] to the Parrot A.R Drone 2.0. In that study, several general facts and file formats were discussed, and the flight path was thoroughly visualized with the help of Google Earth. That approach was found with a high focus upon general technical descriptions of a drone with a forensic perspective. In another research carried out by [8], in-depth forensic analyses were applied to the Parrot AR Drone 2.0, its GPS Edition and its outlying components, i.e., the flight recorder and flight controller. A study in [25] attempted to explore the difficulties that may appear during forensically analyzing UAV/drone. To this end, they decided to explore and evaluate currently used forensic guidelines regarding their efficiency when applied to DRFs analyses. After that, the authors offered their own set of guidelines in this regard, and to end with, they explained the way their guidelines can be effectively implemented when analyzing a drone forensically. As a case study, DJI Phantom 3 drone was used. One of the most important limitations in UAV forensics is the absence of already-confirmed forensically sound tools, which indeed offers a direction for future research. For instance, the next logical step would be the creation of various parsing tools with the capability of analyzing original data and providing legible and dependable information.

Moreover, in the future, UAVs will have the required capacity to be well integrated with radio communication services. As a result, forensic acquisition and analysis of artifacts from radio-communication services can be explored, as well as a lack of standardization towards UAV investigation processes. Attempting to address this observation, a study in [26] proposed an architecture-based approach using the Id-Based Signcryption to guarantee the authentication process and privacy preservation. Firstly, the important elements on which the architecture relies were defined. Secondly, the interaction between these elements was examined to understand how the process works. Then, the proposed authentication scheme was explained in detail. As a result, they used the RFID tags to track drones and the temporary identity for purposes of privacy preservation. A simulation was conducted to calculate the average renewal of temporary identity by varying the time and the drones' speed. Using a similar proposition, a study in [27] attempted to analyze a captured UAV under forensic conditions. A suspected UAV may be captured by security forces with the use of a shotgun (or any other applicable technique) or it may be a device that has crashed into private property. When UAVs are to be subjected to forensic investigations, there is a need for the identification of their software/hardware modules. Then, it is necessary to collect available evidence, provide the chain of custody and analyze the media/artefact loaded on the device. On the other hand, the illegitimate use of UAVs, which is increasingly occurring, shows a legal loophole that exists in the currently applied aviation regulations. This has, consequently, led to a shortage of adequate information and prevailing standards on how the UAV incidents can be investigated. Conversely, a study in [28] explored the potential cyber-physical security threats and attempted to address the existing challenges that can be attributed to UAV security, before UAVs become the prevailing vehicles in future smart cities. Furthermore, the authors suggested a method applicable to the investigation of large-scale cyber-security attack vectors of such systems based on four categories of systems, which are of high importance to UAV operations. Moreover, they explained their impacts in detail and the effective ways to counter such attacks. In another project, arbitrary software was designed and applied by [29] to a locked target to gain access to interior sensors and logs of the device using neutralization and hardening strategies to predict the effectiveness.

A study in [23] proposed an inclusive-based framework for drone forensic analysis, involving both physical and digital forensics. The framework had enough proficiency to be applied to the post-flight investigations of the activities of the drone. In the case of physical forensics, a model was created with the capability of investigating drone components right at the crime scene. Moreover, the authors designed a powerful application that could be implemented in digital drone forensic analysis, centering mainly upon the analysis of the drones' critical log parameters through a graphical user interface (GUI) that was developed with the help of JavaFX 8.0. In another research, Ref. [30] proposed a new Distributed, Agent-based Secure Mechanism for IoD and Smart grid sensors monitoring (DASMIS) scheme. It was designed to run over a hybrid of peer-to-peer (P2P) and client-server (C/S) network architecture with reduced protocol overheads for immediate and bandwidth-efficient communication. In this system, each node is loaded with an initial status and equipped with a python-based agent that is capable of scanning and detecting burned in read-only node- IDs, Node IP Address, node MAC address, system calls made, installed applications, all running system programs and applications and modifications. In addition, it performs data encryption and hashing, and reports changes to other peer nodes as well as to the server sitting in the C&C center. The agent securely authenticates nodes, enciphers the communication and authorizes inter-node access. It prevents and detects attacks such as masquerading, modification and DoS attacks.

Furthermore, the study in [31] conducted a study that was aimed at giving help to whoever is tasked with the generation and analysis, validation and/or optimization of data to trace evidence recovery. For this purpose, the authors elaborated the approach used to solve this problem based on the target fiber retrieval context with the use of self-adhesive tapes. In addition, Ref. [32] attempted to adapt digital forensic processes capable of improving the drone incident response plan through the implementation of the digital forensic analysis process. In that study, more detailed information was provided regarding the developed Drone Forensic and Incident Response Plan (DFIR). The findings showed that the Federal Aviation Administration (FAA) can update the requirements of its Unmanned Aerial Systems (UAS) based on two classifications of UAS. They also comprehensively reviewed the related literature and concluded that it lacked studies focusing upon incident responses and there could not be found forensic analysis frameworks developed specifically for remotely piloted aerials systems. For that reason, the authors made an effort to fill the gap. The electromagnetic watermarking concept was introduced by [33] as a technique that exploits the IEMI impacts for embedding a watermark into civilian UAVs to perform forensic tracking. A small sample of aircraft accident investigators, digital forensics investigators and examined the use of a forensics framework to conduct forensics on a drone [34]. The data analyses that were carried out with the use of the chi-square test of independence did not reveal any considerable connection between the groups of respondents' drone investigations and the methods used to conduct UAS forensics. A study in [35] discussed drone attacks from a different perspective. Their study was mainly aimed at identifying where the SDR board is or can be applied to the implementation of an attack and/or a countermeasure so that current and future risks can be highlighted. As a result, their analysis was mainly centered on two facets one of which was related to targets of the attacks, and the other one to the direction of the attacks. There may be more than one target, which offers multiple possible countermeasures. Targets may include the sensor (mainly GPS), telemetry, remote tele-control, the embedded software, the physical signature (optical, audio, infra-red, electromagnetic and radar) and/or cognitive channel (cognitive scrambling and stealthy communication). The attacks may be directed from ground to drone or vice versa, or even from a drone to drone. The study further proposed an innovative method for quickly and accurately detecting whether a drone is flying or lying on the ground. Such results are obtained without resorting to any active technique; rather, they are achieved through just eavesdropping on the radio traffic and processing it through standard machine learning techniques. According to [35], with effective classifying the network traffic, the drones' status can be properly detected with the help of the widespread operating system of ArduCopter (e.g., several DJI and Hobbyking vehicles). In addition, a lower bound was formed upon the detection delay at the time of applying the above-noted methodology. The proposed solution could discriminate against the drones' state (steady or moving) with roughly 0.93 SR, in almost 3.71 s. A study in [36] evaluates the security susceptibility of two drones, namely Eachine E010 and Parrot Mambo FPV. The former drone was vulnerable to Radio Frequency (RF) replay and custom-made controller attacks, whereas the latter was found susceptible to de-authentication and FTP service attacks. The authors provided a full discussion on both the security susceptibilities of the above-mentioned UAVs and the potential countermeasures that can be taken into action for the aim of improving the resilience of UAVs against probable attacks. A summary of the findings and limitations of DRFs illustrates in Table 2.

Table 2. A Summary of Articles Focused on (DRFs).

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
1.	[37]	Investigation and analysis of both the DJI Phantom II and DJI Phantom III model UAVs.	He discovered that DJI Phantom III includes two types of flight log files, that assist in recover a plethora of data to trace the aircraft back to the owner. This contained GPS and other EXIF data from photos, release points, DJI account information and the owner's name. In addition, explained that experts can create a Secure Shell (SSH) link to the drone and dump the root file system and seize it in real-time utilizing a tool called Skyjack.	It did not concentrate on Phantom III. A lack of a generic process for investigating drones related criminality.
2.	[17]	Testbed model of evidence acquisition from UAVs.	A drone analysis environment can be developed based on the integration of off-the-shelf tools. The tools include Arduino Uno Microcontroller and Raspberry Pi, X-bee Pro 900 HP radio, U-box LEA-6H GPS module, M5 router, A JavaFX API-based GUI and Parallax MS-5607 altimeter module.	Forensic soundness assurance is largely ignored in the platform. A method of ensuring the reliability of the captured remains an open challenge.

Table 2. *Cont.*

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
3.	[16]	A forensic examination of the flight path reconstruction method for DJI Phantom 2 Vision Plus.	Two methods of precise flight data extraction: Ground Control Station memory running on a mobile device and one using EXIF data of recorded media files. Timestamp alteration as a possible anti-forensic approach.	The result cannot be generalized as only one device is presented. Furthermore, the details of the result presented are not given.
4.	[2]	Preliminary digital forensic analysis of Parrot Bebop UAV (capable of 1080p HD footage and 14 megapixels still images, a 2.4 GHz or 5 GHz Wi-Fi band, s, flight distances can extend beyond 2000 m and to a maximum altitude of 150 m).	The location of various forensic artifacts such as flight data (located at the 'internal_000/Bebop_Drone/academy folder), date and time format (for example: 0901_2015-07-1T193919 + 0000_724B2C.pud), serial number (e.g., PI023353423AL23483), Log data.	Only one model of the Parrot Bebop UAV was examined. An extensive study would be required to corroborate the findings for generalization.
5.	[38]	Development of visualization tool for drone analysis.	A tool was developed which integrates CSV and XML-based file format as input, for data visualization. A 3-dimensional view of data collected from AR drone 2.0 was experimentally observed.	The result presents a promising tool that can be enhanced towards a forensically sound visualization and analysis tool. The use of jNetPcap and jPcap further present a platform-independent analysis.
6.	[18]	Drones' vulnerabilities.	His findings confirmed that in cases where drones are hacked and misused by opponents, it can lead to considerable threats. It conducted tests on the benefits of applying drones to an extensive range of situations, from using them as children's toys to applying them as weapons for mass destruction.	Limited on open access sources to conclude the selected topic.
7.	[19]	Drone forensic framework: Sensor and data identification and verification- Specifically, this research analyses the architecture of drones and then proposes a generic model that is aimed at improving digital investigation.	A forensic model was introduced to determine and authenticate a variety of drone components that are available for committing illegitimate actions. It was mainly centered upon the analysis of physical evidence gathered from the crime scenes along with the GPS locations and any multimedia file that may be explored onboard. This research was carried out on five various commercial drones together with their components when captured at crime scenes.	Currently, still, drones have several vulnerabilities. One major issue that has been identified in this perspective is the invasion of privacy and specifically the lack of training to the Law Enforcement Agencies (LEA) on the procedures for conducting investigations for drones.

Table 2. *Cont.*

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
8.	[20]	DROP (DRone Open-source Parser) your drone: Forensic analysis of the DJI Phantom III.	In this research, an open-source tool called Drone Open-Source Parser (DROP) was developed, which was capable of parsing DAT files extracted from the drone's internal storage and comparing them with the TXT files stored in the mobile device that takes the control of the drone. The tool establishes a connection between the device and the user through the correlation of these data.	The best forensic techniques that can be used for acquisition from drones that have been tested stand to be manual extraction of SD cards and disassembling the drone. The main limitation is that the full spectrum of potential data that could be used as digital evidence cannot be extracted from DAT files-owing to the fact that DAT files may delete stored data.
9.	[39]	Mainly Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence. This has been achieved through Digital forensic evidence extraction through the simulation of a UAV scenario that explicitly uses drones.	The authors provided a discussion about the way the GPS coordinates are applicable as location evidence regarding the crimes committed through drones. In this study, the system logs were extracted, and the GPS coordinates were visualized on maps, where web-based third-party platforms were applied to plotting the flight paths.	The percentage amount of digital information that was extracted stood at 50%, as a result, it is highly not sufficient enough to create a concrete hypothesis for litigation purposes.
10.	[21]	An investigation into the effect of surveillance drones on textile evidence at crime scenes.	The authors examined the impacts of a quadcopter's downwash to understand whether it can influence the retention of textile evidence in crime scenes. Yarn retention on a range of floor types was recorded after a drone flypast at various heights and taking off at pre-set distances from the evidence region. This study was carried out to assist the police forces who wish to make use of a quadcopter drone surveillance in the future to well maintain the integrity of scenes by adhering to or flying above any minimum "safe height" and "safe distance", which have been determined in advance.	The distance between the point of taking off of the quadcopter and the evidence affects the quantity (number) of evidence that can be explored. There is also needed to adopt the use of microscopic fibers for additional tests.
11.	[22]	Drone Forensic Investigation: DJI Spark Drone as A Case Study.	The paper was aimed at comparing and verifying the correlation of the flight data amongst the drone, SD card and mobile phone. To facilitate criminal investigations, a connection can be established between the drone and the suspect.	Analysis of flight logs that are based on temporal analysis (timestamp, GPS coordinates and number of files) did not show any association to evidence of the drone, the SD card and the mobile device.

Table 2. *Cont.*

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
12.	[24]	Drone Forensics: Digital Flight Log Examination Framework for Micro Drones.	The authors attempted to analyse the key log parameters of the autonomous drone. They proposed an inclusive drone-forensics-related software architecture with preliminary results. The proposed software was expected to make available a user-friendly graphical user interface (GUI) that can make users capable of extracting and testing the onboard information of flight. This paper proposed a new tool applicable to the investigation of criminal cases related to drones.	Several drones do not have the capability of logging events. In addition, the unavailability of drones to the investigator due to customization is a challenge for drone forensics. Consequently, it is not easy to identify the drone user which is a challenge unless they are registered to the drone manufacturer.
13.	[15]	Drone Forensic Analysis Using Open-Source Tools in The Journal of Digital Forensics, Security and Law.	The authors made use of open-source tools such as ExifTool and CsvView for the aim of extracting artifacts from mobile applications of drones with the help of mobile forensic techniques. They employed Kali, a Linux distribution and Windows as their forensic workstation to carry out a forensic analysis upon two drones: A.R Drone and DJI Phantom 3. For the visualization of the flight path data, open-source tools such as GeoPlayer were employed in this study.	From the propositions in this research, forensic analysis of drones needs a polymathic approach that can simultaneously be able to adapt to the voluminous embedded and mobile environments that can be encountered. There is also needed to integrate other mobile platforms such as IOS and Windows Phones so that the approaches can easily be integrated into commercial forensic toolkits to benefit the digital forensic community.
14.	[25]	Drone Forensics: Challenges and New Insights.	The authors in this paper applied digital forensics to the Parrot A.R Drone 2.0. They provide a discussion on several general facts and file formats and then attempted to visualize the flight path with the help of Google Earth. The approach provided in that study was centered further upon general technical descriptions of a drone from a forensic point of view.	Based on the challenges that have been identified in this paper, reconstructing a sequence of events from A.R Drone based on the history of the flight path poses a challenge in instances when the EXIF data does not possess GPS attributes. In addition, it is a challenge when it comes to identifying the owner of the drone-based on the controller's ID based on memory partitioning.
15.	[40]	Unmanned aerial vehicle forensic investigation process: DJI Phantom 3 drone as a case study.	The authors presented the challenges that may appear when working with UAV/drone forensics. Afterward, they made some evaluations on currently applied forensic guidelines, regarding their efficiency in UAV/drone forensic investigation. Then, the authors offered their own set of guidelines for UAV/drone investigations and attempted to show the way their guidelines can be well applied to guiding a drone forensic investigation with the use of the DJI Phantom 3 drone as a case study.	There is a lack of validated tools that can collect forensically sound digital evidence. To analyze original data in this context a parsing tool could be used to provide results that can be reliable.

Table 2. *Cont.*

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
16.	[26]	Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV.	The authors in this study designed and run arbitrary software on a locked target to gain access to interior sensors and logs. The relevant impacts were obtained, which provided the possibility for both neutralization and hardening strategies and also predicting the effectiveness of the protection offered by such a solution.	During data collection, one may need to acquire access to the observable data, and, unfortunately, one needs to physically interact with the smartphones during the testing or rely on local logs from the UAV. In addition, the huge access logs are contained in the SD card which partially many need decoding, hence not suitable for real-time analysis purposes.
17.	[26]	Unmanned Aerial Vehicle Digital Forensic Investigation Framework.	This paper was centered on forensically analyzing a captured UAV. The UAV could be captured by security forces using a shotgun (or any other anti-UAV technique) or it could be a UAV that has crashed into private property. For the implementation of forensic analysis on a UAV, there is a need for identification and investigation of its hardware and software components. Moreover, there is a need to gather required evidence, provide a chain of custody and analyze media/artifacts.	Given the increased and massive usage of UAVs, there have been several cases of illegal usage of these devices. As a result, this identifies a loophole that shows a lack of aviation regulations and forensic investigation standards of potential incidents.
18.	[24]	Autonomous Arial Vehicles in Smart Cities: Potential Cyber-Physical Threats.	This study was aimed at the exploration of the potential cyber-physical security threats and the challenges in this regard before drones are accepted as ordinary vehicles in future smart cities. The authors introduced a new method for investigating on a large scale the cybersecurity attack vectors of such systems based on four classes of systems that are of high importance to AAV operations, and their effects and the way to take an effective countermeasure to such attacks. After that, the authors summarized the countermeasures that need to be taken into action aiming at guaranteeing the systems' safety.	Given that only four distinct potential attack vectors, it is important to derive these vectors from multiple sources so that the options of widening such autonomous systems in the wake of an attack. This consideration is pivotal even though it may lead to multiple attacks. Consequently, there is a need for the AAV to recognize anomalies and make an emergency stop on numerous occasions Petit, J. and (Shladover, 2015).
19.	[27]	Privacy preservation and drone authentication using ID-Based Signcryption.	This paper proposed an architecture using the Id-Based Signcryption to guarantee the authentication process and privacy preservation. First, the authors defined the important elements that the architecture relies on. Second, they took into consideration the interaction between these elements to understand how the process works. Then, they presented the proposed scheme of authentication in detail. For this purpose, the RFID tags were used to track drones and the temporary identity for privacy preservation. A simulation was performed to calculate the average renewal of temporary identity by varying the time and the drones' speed.	Given that this is a preliminary architecture that assigns an ID to drones based on temporal identity the algorithm needs to be able to give security communication about the effectiveness of the simulations and to check whether there exist secure communication of the identities between the drones.

Table 2. *Cont.*

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
20.	[28]	A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework.	An inclusive drone forensic framework was introduced in this paper, which involved both physical and digital forensics. It was found applicable to the post-flight investigation of drones' activities. In the case of physical forensics, the authors introduced a model with the capacity of examining the drone components at the crime scene. In addition, the authors presented a powerful digital drone forensic application focusing primarily upon the analysis of the critical log parameters of drones through a graphical user interface (GUI) that was developed with the help of JavaFX 8.0.	There is a limitation of the drones used (DJI Phantom 4 and Yuneec Typhoon H) not being able to log events. In addition, the drone needs to be there physically for the forensic investigator. Furthermore, it is a challenge for drones that store data in smartphone apps because of the difficulty of data acquisition. Additionally, the lack of standards on drone file formats also analyzes an arbitrary drone hard. A final limitation is the identification of the drone user-it is difficult if not registered before flying the drone.
21.	[41]	An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring.	In this study, a new Distributed, Agent-based Secure Mechanism for IoD and Smart grid sensors monitoring (DASMIS) scheme was proposed. It is designed to run over a hybrid of peer-to-peer (P2P) and client-server (C/S) network architecture with reduced protocol overheads for immediate and bandwidth-efficient communication. Each node is loaded with an initial status and equipped with a python-based agent that is capable of scanning and detecting burned-in ready-only node-IDs, Node IP Address, node MAC address, system calls made, installed applications, all running system programs and applications and modifications. In addition, it performs data encryption and hashing, and reports changes to other peer nodes as well as to the server sitting in the C&C center. The agent securely authenticates nodes, enciphers the communication and authorizes inter-node access. It detects and prevents attacks such as masquerading, modification and DoS attacks.	It is imperative to note that in this context, drones and the smart grid are portrayed to be prone to attacks against availability, integrity and privacy, given that drones can be hijacked, weaponized or stolen. Denial of Service (DoS) may be imminent or it can be perpetuated on drones which may render the information being gathered to unauthorized users.
22.	[30]	The effect of tape type, taping method and tape storage temperature on the retrieval rate of fibers from various surfaces: An example of data generation and analysis to facilitate trace evidence recovery validation and optimization.	The findings of this study were expected to give help to those whose task is producing and analyzing data, aiming to validate and/or optimize the trace evidence recovery. The objective was achieved by adopting a new approach to this problem in the context of target fiber retrieval with the use of self-adhesive tapes.	Experiments that have been conducted are mainly represented based on three clusters that are focused on the median and interquartile range of fiber retrieval. There is, however, a degree between conditions overlaps in the apparent data. The study also used sandpaper to abrade the surface of the donor fabric from which the target fibers were obtained, this could have damaged the fibers that were used for the experiment.

Table 2. *Cont.*

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
23.	[31]	Drone Disrupted Denial of Service Attack (3DOS): Towards an Incident Response and Forensic Analysis of Remotely Piloted Aerial Systems (RPASs).	The authors in this research were focused on the adoption of digital forensic procedures that could improve the drone incident response plan through the interpretation of digital forensics analyses. This study provided more detailed discussions about the developed Drone Forensic and Incident Response Plan (DFIR). Federal Aviation Administration (FAA) can update the requirements of its Unmanned Aerial Systems (UAS) based on two classifications of UAS.	The authors identify the need for improving the DRZF tool to incorporate features such as the automatic interpretation of the drone's black-box for purposes of conducting digital forensic reporting. In addition, the need for incorporating incident response plan and pre-incident and post-incident measures is of dire importance for this tool.
24.	[32]	Electromagnetic Watermarking: exploiting IEMI effects for forensic tracking of UAVs.	In this paper, the concept of electromagnetic watermarking was discussed, which is a technique for the exploitation of the impacts of IEMI to embed a watermark into civilian UAVs to perform forensic tracking.	Given that watermarking offers the most effective way to put the information to the targets that do not seem to be cooperating, this opens a new area worth exploring. In addition, there is a need to explore the diversification of other applications so that other contexts apart from forensic tracking can be explored. Lastly, this research also shows the need for generalizing this concept to various fault injection vectors.
25.	[33]	An Approach to Unmanned Aircraft Systems Forensics Framework.	This research surveyed a small sample of digital forensics investigators and aircraft accident investigators and the way they utilize the forensic framework when applying forensics to a drone. Data analysis with the use of the chi-square test of independence showed no considerable relationship between the drone investigations of the respondents and the methods applied to UAS forensics.	The quantitative explanatory correlation research identifies the lack of standardization and lack of quality controls as a major issue for the UAVs and that the digital forensic investigators for the UAVs in most cases will only adopt ad hoc processes as opposed to industry best standards. Scientifically this goes against the Daubert Rules/standards on the admissibility of digital evidence (Pipoly, 2011).

Table 2. *Cont.*

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
26.	[34]	Detecting Drones Status via Encrypted Traffic Analysis.	The authors in this paper proposed an innovative method for detecting quickly and accurately whether a drone is either flying or lying on the ground. These outcomes were attained without resorting to any active technique; rather, the radio traffic was eavesdropped on and then processed through standard ML techniques. It was confirmed that network traffic classification is effectually applicable to detecting the status of drones using the prevalent operating system of ArduCopter (such as some DJI and Hobbyking vehicles). In addition, the authors offered a lower bound on the detection delay when implementing the proposed method. The solution proposed in this study was proved capable of discriminating against the drones' state (whether they are steady or moving) within approximately 3.71 s and an SR of roughly 0.93.	Results in this context are achieved through eavesdropping on the radio traffic and processing it through machine learning. It may be important if many attacks can be used so that the machine learning model can be able to predict the likelihood or probability of future attacks either as targeted or unintentional attacks.
27.	[36]	Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles.	This study was mainly centered on the evaluation of the security susceptibilities of two drones, namely Parrot Mambo FPV and Eachine E010. The former was found susceptible to de-authentication and FTP service attacks, whereas the latter was found susceptible to radiofrequency (RF) replay and custom-made controller attacks. The authors not only exploited the security vulnerabilities of the two UAVs but also discussed the potential countermeasures for the aim of enhancing the resilience of UAVs against the identified attacks.	There is a need for exploring the drone functionalities and vulnerabilities for GPS and jamming attacks. In addition, there is an emphasis on identifying different attacks such as privilege escalation attacks when the UAVs Operating System is modified, coupled with countermeasures that can mitigate this process.
28.	[35]	Risk assessment of SDR-based attacks with UAVs.	The authors discussed drone attacks from a different perspective. Their research was mainly aimed at identifying where the SDR board is or can be employed for the implementation of an attack and/or a countermeasure; this way, they attempted to highlight current and future risks. As a result, the analysis is focused on two facets: the first facet is related to the targets of attacks, and the second one is related to the direction of attacks. The attacks may have more than one target, thereby having multiple countermeasures. The attacks may include telemetry, remote tele-control, the physical signature (optical, audio, radar, infra-red, electromagnetic, etc.), sensor (mainly GPS), cognitive channel (cognitive scrambling, stealthy communication, etc.) or embedded software. The attacks can be directed from ground to drone, or vice versa; it can be even from drone to drone.	The general threats in UAVs start from the ground to the drone and the core challenge is the use of the Software Defined Radio (SDR) that are embedded in the UAVs. SDR is used as a platform for attacks and for countermeasures which should be explored in detail for possible upcoming threats that are focused on improving security.
29.	[36]	Forensic analysis of the Parrot AR Drone 2.0 GPS Edition and its peripheral components.	The authors discovered that it is possible to recover GPS data and media files containing EXIF data from both the Parrot AR Drone 2.0 and the flight controller.	In contrast with these results, only media files containing EXIF data were retrieved from the Flight Recorder, and still difficult to identify the definitive owner of a UAV.

Table 2. *Cont.*

ID	Ref	Focus	Synthesis of the Study	Limitations/Observations Made
30.	[42]	Anti-drone system.	Provided a comprehensive overview of the technologies utilized for drone surveillance and the existing anti-drone systems. The authors proposed an anti-drone system at Zhejiang University, named ADS-ZJU, which combines multiple passive surveillance technologies to realize drone detection, localization and radiofrequency jamming.	No forensic model was developed. However, the content presents useful content which can be used to substantiate some technical component of drone forensics.
31.	[43]	Techniques of detecting and tracking UAV.	The authors provided a unified review of the techniques for detecting, tracking and interdicting small unauthorized UAVs around restricted areas.	The review is limited to some technical components, which lack a forensic model.
32.	[44]	Amateur Drone Surveillance System.	The authors developed an amateur drone surveillance system based on cognitive IoT.	IoT-based surveillance systems could provide a useful hint for forensic modalities. However, the study failed to develop any forensic model.

3.3. Phase 3: Findings and Limitations

The detailed review of the selected articles identified four thematic descriptions as shown in Figure 3 namely: (1) forensic analysis, (2) non-forensic analysis, (3) forensic framework, (4) application in forensic analysis, suffice it to note that there seems to be a growing body of research in DRFs which further highlight the need to draw urgent attention to areas of potential interest, and potentially detrimental impact if not investigated. In this section, the four categories are explained in detail.

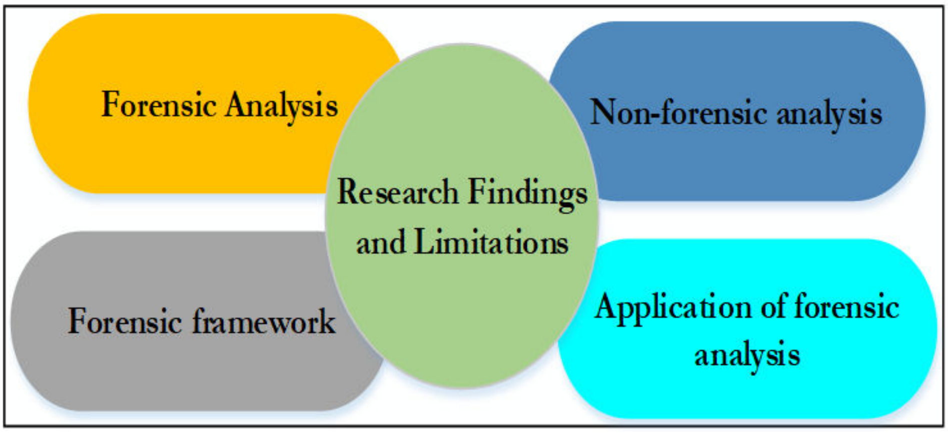
Forensic Analysis
Non-forensic analysis
Research Findings and Limitations
Forensic framework
Application of forensic analysis

Figure 3. Thematic Depiction of the Drone Forensics Models.

- Forensic analysis: Has been a subject of disputes among researchers, where researchers have in many instances explored diverse dimensions in the quest of assessing the security measures, attacks and the countermeasures, and to understand how to prevent such activities [1,27,30,34–37,40]. Notably, relevant research has focused on the techniques that can be used to analyze the compromised devices such as [1,2,17,19–21,23,26,28,36–39]. The common approach is to analyze the stored data in the device from a digital forensic perspective. The use of multi-staged authentication through different processes to increase the security of the drone has also been explored significantly. Furthermore, studies have applied encryption applied and authentication with additional steps of identifying important elements and their inter coordination [25]. Different tools have also been utilized to develop in the development of reliable techniques, which include Drone Open-Source Parser (DROP), Exifpool, csvView and Geoplayer. The DAT files of the system, operating system logs, device controller logs and flight status logs are also used to identify the potentials for improving the results of forensic analysis.

- Non-Forensic Analysis: is directly applied to drone forensic analysis. However, this type of analysis provides indirect assistance to improve the outcome for the later phases. These are mainly used to visualize the flight status and improve the communication channel and the communication between the devices. Such information is helpful to visualize the status of the drone. These types of analyses use the controller data and the drone log file for visualization.
- Application of Drones: As a result of literature exploration, it is imperative to highlight that there are diverse application areas of drones. Most application areas had a focus on the following aspects: Toys-drones, surveillance purposes, weapons of mass destruction, disaster management activities, agriculture, delivery services and criminal investigation and textile industry as well.
- Digital Forensic Framework: Guidelines and frameworks that can help to improve the performance of forensic investigations such as [21,42,45,46] have been explored. In addition, a framework that can deal with both the hardware and software of the drone have been developed [26]. Those propositions went an extra mile to explore artifacts, the chain of custody which serves as an important aspect in digital forensic analysis. Furthermore, the study explored a framework that has a focus on post-flight analysis as a key aspect that can be of importance during forensic analysis [23].

4. Open Research Problems

Whilst research directions have mainly focused on investigating the functionality and the physics of UAVs, fewer researchers have investigated the feasibility of developing models that can be integrated into a standardized approach. This is a major limitation that requires urgent attention. Models that focus on drone investigation, legal frameworks for jurisdictional settlement as well as frameworks on legal cooperation fall within the techno-legal discipline. Such a model would have the potential to develop a mechanism needed to actualize the defense against drone attacks, given that malicious users tend to prey on the vulnerabilities based on the respective jurisdiction.

Additionally, models that attempt to offer explicit guidance on technical specification investigation and device fingerprinting remain a major backbone for effective drone investigation. Given the potential for the proliferation of substandard (as well as brand imitation) drones, there is an urgent need for studies that can provide a method of device correlation and fingerprint for the identification of the manufactural of drones. The forensic community will greatly benefit from methods that can be used to reliably corroborate a given assertion on the name, make and model of a given drone without ambiguity. Such studies would, however, be required to further provide a scientifically proven basis for a given conclusion. Device fingerprint, for instance, can rely on the specific frequency emitting by each radio device. The research community can also benefit from studies that attempt to articulate commonalities among UAVs to provide metrics for the face-identification of UAVs. This can help to reduce or profile a given UAV during incident response. A certainty, however, is that crimes that seek to employ the advantage of the drone will continue to surge, while UAV manufacturers will eventually seek to mass-produce drones with complex functionalities. These peculiarities among other unexplored areas have opened the need to explore open and future challenges in UAVs that are discussed further on.

Basing our focus on the popularity that has been realized as a result of the usage of UAVs, the existing or ever-rising security issues still show the potential of warranting a digital forensic investigation. As mentioned previously in this paper, there exist several challenges, more importantly, analyzing the flight path of drones, timestamp source and destination, and the manufacturers-which play an important role at this stage. This requires one to have efficient and effective tools and techniques that can be used to forensically identify the anatomy of the drone. Among these requirements, we also take note of the fact that there may exist legal challenges due to the absence of well-documented or acceptable investigation approaches and standards that are in a position of providing actionable digital evidence that can be used to link a suspect with a potential digital crime.

There also exist formidable constraints pertaining to real-time data capturing for drones based on their mobility aspects, for example, it would pose a challenge for the UAV to capture geographical data in the 3D aspect even though forensic techniques may be employed as a post-event response aspect. While it is evident according to existing studies that using a variety of mobile devices for purposes of collecting data using UAVs in a controllable environment could be a step towards forensic techniques, it is also important to note the fact that several constraints exist concerning long-lasting transmissions from sites/stations. This is owing to the technical complexity of UAVs and how effective the various devices may collaborate with the presence of obstacles for purposes of getting optimal real-time data gathering.

That notwithstanding, there is still an open challenge as far as how the drone is customizable, which in real context brings about complex issues when conducting digital forensic investigations [1]. While these customizable aspects can tamper with the design of the drone, it is imperative to note that this is still an open problem that is worth addressing at the time of writing this paper. In addition, given the quick proliferation of drones, the Law Enforcement Agencies (LEAs) still lack proper training on the use of drones, which also presents an open challenge when executing digital forensic investigations.

We stress the fact that a drone may interact with a diverse and complex environment, such as a smart-connected environment, and the complexity that may be involved may sometimes pose a challenge for investigation. The dynamically changing environment may, in most cases, act as a threat landscape hence complicating the concept of attribution.

5. Proposed Unified Forensic Investigation Model for UAV

Based on the observation presented in the previous section, there seem to exist, diverse investigation models, processes, tools and frameworks for UAV forensics. These models are, however, defined within the context of the specific investigation, as summarized in Table 2. Moreover, for a forensic domain to scale through the legal scrutiny, and corroborative processes, a generally accepted structure is required. There are only two proposed investigation models [18,26] for the UAVs in the literature. These proposed models have a complicated configuration and are greatly developed on a platform-specific basis. Additionally, both frameworks failed to explicitly define forensic soundness as a core component for the forensic investigation process. Requirements such as the assurance of the chain of custody, and the provision of a chain of evidence are core factors that can impact the admissibility of any investigation. As a step towards addressing this limitation, this study further provides a generalizable investigative model for UAV forensics. The proposed model is shown in Figure 4. It consists of three main investigation phases which are: preparation phase (pre and post-incident); data acquisition phase; and data analysis phase. Each phase has combined most and common activities and tasks of the existing UAVs models where each phase is further elaborated:

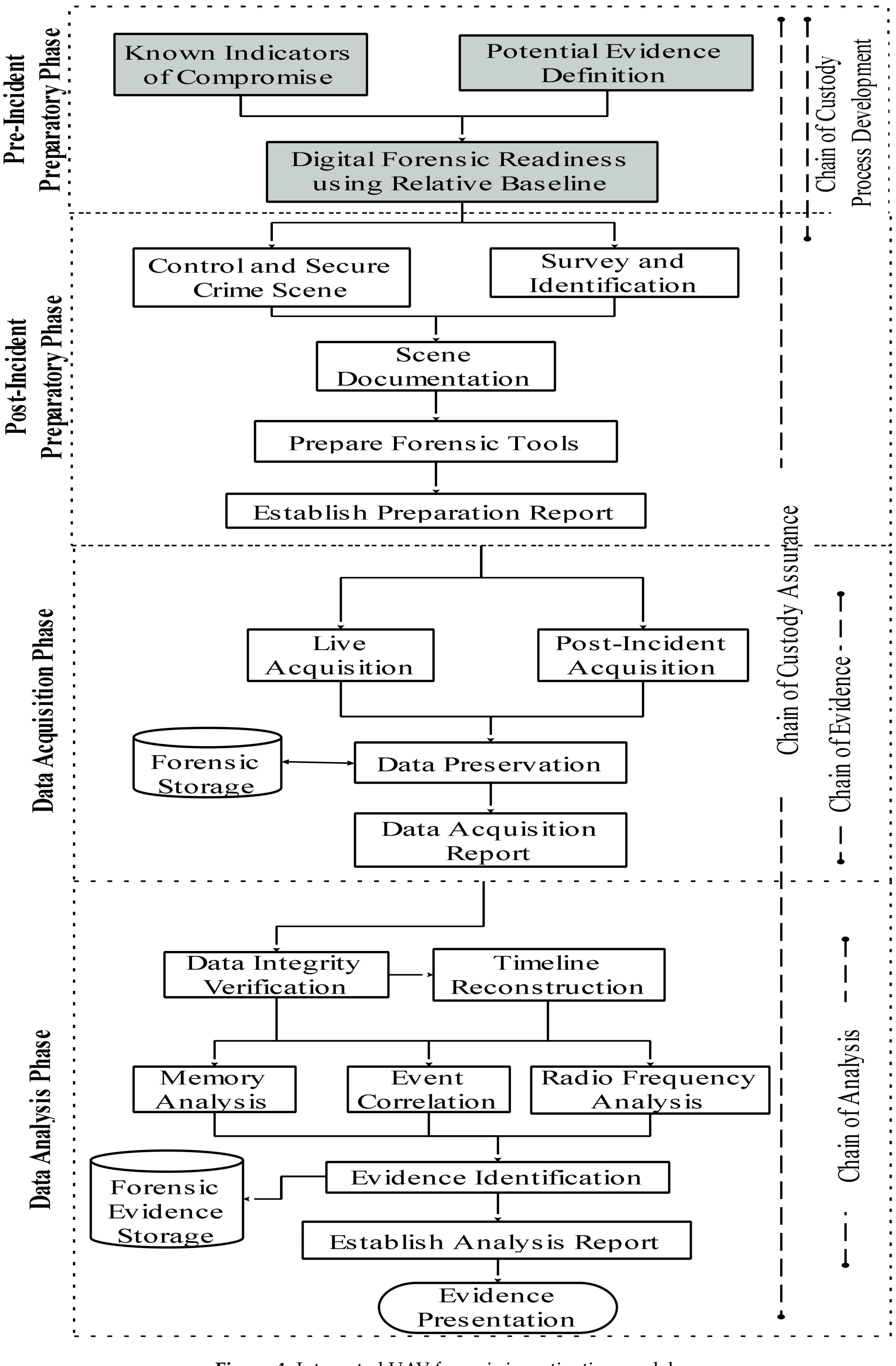
Pre-Incident Preparatory Phase
Known Indicators of Compromise
Potential Evidence Definition
Digital Forensic Readiness using Relative Baseline
Chain of Custody Process Development
Post-Incident Preparatory Phase
Control and Secure Crime Scene
Survey and Identification
Scene Documentation
Prepare Forensic Tools
Establish Preparation Report
Chain of Custody Assurance
Data Acquisition Phase
Live Acquisition
Post-Incident Acquisition
Forensic Storage
Data Preservation
Data Acquisition Report
Chain of Evidence
Data Analysis Phase
Data Integrity Verification
Timeline Reconstruction
Memory Analysis
Event Correlation
Radio Frequency Analysis
Forensic Evidence Storage
Evidence Identification
Establish Analysis Report
Evidence Presentation
Chain of Analysis

Figure 4. Integrated UAV forensic investigation model.

Preparation phase: this phase is further categorized into (pre-incident and post-incident preparation) phases. The pre-incident phase involves attempts to pre-empt incidents by extracting a baseline device configuration before any approved operation. Careful attention is further required in this phase towards the development of an acceptable forensic process. This includes the establishment of the protocol to follow to ensure the chain of custody. This could include the use of an appropriate cataloging process, procurement of forensic storage apparatus, as well as the defined protocol for evidence handling. On the other hand, the post-incident phase involves several tasks and activities to prepare UAVs for investigation. These are explained thus: Known Sources of Indicator of Compromise (IoC): these are input sources to the pre-incident phase where a forensic investigator is required to identify potentially reliable sources where indicators of drone compromise have been identified and documented. Here, repositories from open-source intelligence can be leveraged. Potential attack vectors can be identified to instantiate the Readiness process for investigation.

- Potential Evidence Definition: Defining what could make up evidence for drone forensics is a nontrivial process that could, however, be difficult when an incident has occurred. Therefore, the need for an iterative potential evidence definition could be a core step towards enhancing the time and efficiency of drone forensics. This is particularly important in DRFs to prevent poor evidence collection. The proposed integrated UAV investigation model is an extension of the respective frameworks presented in Figure 4.
- Digital Forensic Readiness (DFR) using Relative baseline: Forensic readiness has been identified within the digital forensic [40,47–50] domain as a veritable tool for enhancing evidence reliability and availability. The concept of relative baseline involves the process of comparing the forensic parameters of one drone to other similar drones to establish baseline data within the drone, before drone operations. A relative baseline can, therefore, address contextual discrepancies by identifying the contextual components of a drone before drone operation. This process receives input from the known indicators of drones/UAV device compromise (IoC) and the iterative potential evidence definition process. Based on these inputs and the underlying functionalities, a DFR can be established.
- Control and securing the scene: Approaches to preventing the alteration of the pieces of evidence and protection of the crime scene from illegal access are the main purpose of this task. During this task, the examiner should take care of any equipment fallen from the UAV during the occurrence. In addition, preserving evidence from being modified is important in this task. Thus, examiners are accountable for the control of the area by identifying the borders of the incident and managing the collected crowd over there. In addition, the protection of UAV equipment at the scene should be guaranteed.
- Survey and Recognition: This task includes a preliminary examination performed by the examiners for assessing the scene, discovering possible resources of evidence and preparing a proper search strategy. In a complicated situation, this may not be easy. In the case of UAV, the most important resources of evidence excluding the device itself are flight data (log files), sensor parameters (GPS coordinates), root file systems, ground control techniques, station memory (internal storage), timestamps, OS, file formats, SDR board and the cognitive channels. Assess the UAV at the scene to verify whether any specialist help is needed in handling the scene. Recognizing people in the scene and organizing initial interviews are very valuable. The owners of the UAV can give useful data such as the aim of the UAV, security schemes, numerous applications appear in the UAV, usernames, passwords, encryption details.
- Documenting the Scene: In this task, the investigators should document the crime scene, as well as take pictures, drawings and mapping of the crime scene. All the UAV's devices at the crime scene should be snapped [51].
- Prepare forensic tools: the proper and trusted forensic tools must be prepared.
- Establish Preparation Reporting: in this step, the investigators are required to prepare a report which includes whole preparation phase tasks.

- Presentation: The presentation task is the last stage of a digital forensic investigation. All tasks produced during the whole investigation stage should be described in detail. A report should be arranged that introduces all pieces of evidence about the incident.

Data Acquisition Phase: this phase is used to acquire the volatile and non-volatile data from the UVA. Interest in this section is the concurrent process of a chain of custody, and a chain of evidence. It consists of five tasks which are:

- Live Acquisition: A live acquisition is a kind of data acquisition that occurs when the UAV OS is operational [52]. Here, live evidence should be acquired/collected by investigators as soon as possible to avoid losing data. The emphasis in this process will include both volatile and non-volatile data sources. Data, in this case, can include memory data acquisition, RF signal capture from Wi-Fi and other wireless communication devices, geolocation data, as well as interactivity events.
- Post-Incident Acquisition: This involves a dead acquisition process that involves copying data from the UAV OS being investigated while the UAV is not operational [14]. Data sources within this process include memory and other event logs within the UAV. Data in this section is primarily non-volatile.
- Data Preservation: It is used to protect the integrity of the evidence acquired from the UAV, both volatile and non-volatile.
- This step aligns closely with the chain of evidence protocol, as well as the use of hash functions for integrity verification. Data Acquired in this step is further stored in a forensic repository where the corresponding hash digest is also stored. A read and write access control mechanism can be integrated into this process, with an appropriate access log, as complementary content that can be integrated into the chain of custody and evidence process.
- Establish Data Acquisition Report: In this step, the investigators are required to prepare a report which includes whole acquisition phase tasks.

Data Analysis Phase: This phase is used to analyze the UAV data and reveal the (cause of the) crime. A further forensic composition of this phase is the chain of analysis. Here, an investigator would be required to ensure a repeatability, and transparency analysis process. This is contrasted to a black box analysis process where the methodology and processes followed in the analysis process are not repeatable by a third party. This phase comprises six tasks as shown in Figure 4. These tasks are further explained thus:

- Data integrity verification: this task is used to check the validity of the collected data. If the collected data is damaged, the investigators are required to re-acquire the data. Data from the forensic repository is used as input to this phase. The integrity verification process can include a bit-by-bit stream copy of the acquired data, and a corresponding comparison of the new hash digest with the existing hash digest in the forensic repository. This process can be expanded to also include the event log verification as well.
- Timeline Reconstruction: upon a valid data integrity verification, this task can be carried out. This task is used to rebuild the timeline of the UAV events and reveal the evidence of the crime. Special emphasis is expected to be taken in this step as the accuracy of the entire investigation process hinges on the degree of 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.
- Data Analysis: These steps can contain the analysis of the diverse data sources from the UAV. For simplicity, this study presents the analysis to entail memory analysis, event reconstruction and radiofrequency analysis. Radiofrequency fingerprinting is also an example of a potential analysis that can be carried out in this step.
- Evidence Identification: in this task, the investigators would be required to identify the evidence and provide a detailed explanation. This step will answer the question of

Who, What, When, Where and potentially, why based on the data. who is the criminal? What time did the crime happen? How did the crime happen?

- Establish Analysis Report: in this step, the investigators are required to prepare a report which integrates the entire analysis phase. Furthermore, the investigator would be required to justify the chain of evidence and chain of custody of the data. This is considered a critical component of this analysis process, as a verifiable process is necessary during litigation.
- Presentation: The presentation task is the last stage of a digital forensic investigation. All tasks produced during the whole investigation stage should be described in detail. A report should be arranged that introduces all pieces of evidence about the incident.

The proposed framework given in Figure 4 depicts a methodical process through which a digital forensic readiness mechanism [47,53,54], can be implemented for drone forensics. However, the implementation feasibility would typically depend on the type of UAV, and the associated technologies, as stated in [55,56]. Characteristics such as UAV performance, space occupation, payload capacity, computational capabilities, navigation precision, data transmission reliability, as well as the legal regulatory frameworks in the cyber ecosystem are key criteria for implementation consideration. The data acquisition phase, for instance, can be implemented as a standalone (or integrated) platform of integrated tools, while ensuring the chain of evidence, as well as the chain of custody. Tools that can harness wireless signal, tools that be used to extract memory information and reconstruct content from a UAV. Such a platform would further require the integration of an integrity assurance mechanism. For instance, the implementation of SHA-256 hash algorithm for all acquired data and all stages of acquisition. In addition, automation processes can be used to formalize the generation of a forensically sound report. A standalone acquisition platform can be used as a plugin module to other platforms.

However, when such a platform is developed as an integrated acquisition platform, graphical interfaces for forensic analysis would be required. Forensic analysis tools typically contain a self-integrity checker, where a proper chain of analysis can be ensured. Ensuring the integrity of the data contained in the UAV in a posthumous investigation would require a validation process that can satisfy the forensic requirement. As highlighted in the data analysis phase of the proposed investigation model, the content of the memory, as well as some potential radio frequency data of the UAV are core components of the analysis process. Processing of radio frequency data could further require spectral analysis, and potentially the application of machine learning algorithms for pattern identification, extraction and matching [57,58]. Another aspect of the UAV data is the integration of GPS coordinate information. Given that such data could lead to a big data problem, the implementation process could therefore leverage diverse modules of data analytics and visualization. Data visualization can also be used to generate an intuitive timeline reconstruction and event correlation. Similar to the acquisition phase, the analysis could also use a hashing algorithm for the integrity verification process. The developed tool can be designed to ensure that every human action on the system is documented for report generation. For example, studies in [59–61] identified core requirements for the development of such an application. The timeline analysis process was incorporated in the tool developed in [59] thereby ensuring the admissibility of any analysis carried out on such a tool.

6. Comparison of Proposed Model with Existing DFR Models

Given the observed challenges, it is evident that the potential acceptability of the collected evidence in existing drone forensic models lacks adequate coverage. Drone forensic investigation must follow a standard of evidence acquisitions for its admissibility in litigation. Thus, the proposed model, combined with the integration of best procedures of existing models, will not only provide law enforcement organizations a proactive and reactive approach against drone-related criminality but will also lead to potentially successful prosecution processes. The proposed integrated model consists of three abstract phases: the preparation phase, data acquisition and data analysis phase. Each phase has several activities and tasks used to identify, detect, analyze, document and present drones' crimes. Comparing to the existing DRF models as shown in Table 3, the proposed model has several advantages which are:

1. The proposed model offers full processes to perform a digital investigation on the drone's devices, where are the existing models specific and concentrate on technical perspective.
2. The proposed model provides a preparation phase that consists of two new processes (pre-incident and post-incident). Furthermore, only the proposed model is the only model that is providing this step among all existing DRF models.
3. Provide coherent as well as the fundamental model.
4. The stream of data in the investigation process is clear.
5. Tools can be used for the examination of evidence.
6. The proposed model is the integration of several abstract processes in an intelligible manner.
7. Suitable for gathering the evidence from the live and dead drone.
8. The proposed DRF model integrates the advantages taken by previous models. It has been defined well in terms of meaning, activities and tasks.
9. Simplify common communication amongst different DRF domain practitioners through a common representation layer that includes all the processes, concepts, tasks and activities that must exist in the DRF field.

Table 3. Comparison of the proposed DRF model with existing DRF models.

Proposed DRF Model		**Existing Models**
Phase	Sub-Phase and Tasks	
Preparation	Pre-Incident ✓ Knowing indicators of compromise ✓ Potential evidence definition ✓ Digital forensic readiness Post-Incident ✓ Control and secure crime ✓ Survey and identification ✓ Scene documentation ✓ Prepare forensic tool. ✓ Establish preparation report	Uncovered
Data Acquisition	✓ Live Acquisition ✓ Post-Incident Acquisition ✓ Data Preservation ✓ Forensic Storage ✓ Data Acquisition Report	Covered
Data Analysis	✓ Data Integrity Verification ✓ Timeline Reconstruction ✓ Memory Analysis ✓ Event Correlation ✓ Radio Frequency Analysis ✓ Evidence Identification ✓ Forensic Evidence Storage ✓ Establish Analysis Report ✓ Evidence Presentation	Covered

7. Discussion

From a pragmatic perspective, the usage of UAVs has significantly increased in the recent past, however, it is also important to highlight that there exists illegal use of UAVs and this has necessitated the exploration of forensic techniques. Relevant and most recent literature that has been explored throughout this paper has found that 29 models that have been identified have shown the need for conducting UAV forensics for the different types of drones. In addition, research has shown that to achieve effectiveness in drone forensics, the OS and the hardware of the drone plays a crucial role in the extraction of relevant forensic data that can be used during digital forensic investigations.

Notably, the fast advancements in the field of digital forensics, particularly drone forensics, show that there is also a dire need for conducting forensic investigations due to ever-rising crimes such as privacy invasion and other illegalities/criminalities. These, among other digital crimes, show the need of incorporating the LEAs and the digital forensic experts in this process. While this study has concentrated on reviewing existing drone forensic models, it was also suitable to propose an integrated model that addresses the challenges from a proactive approach. This study has been able to propose a forensic model that integrates UAV investigations with phases (Preparation phase, Data acquisition phase and Data Analysis phase) which upholds the chain of custody concurrently with the investigation process [57,62]. Important to note, is the fact that this proposed integrated UAV model is not specific to any manufacturer or type of drone, however, it could still be adopted and utilized from a generic standpoint for purposes of investigations. This is considered essential for drone forensics given the inexistence of the unacceptable or standardized UAV Forensic model at the time of writing this paper.

Consequently, from this study, an investigation of drone forensic models has been conducted and it has mainly been inclined on the focus of the drones, the existing propositions, limitations and observations from the selected studies (see Tables 1 and 2). The following aspects have been unmasked as important when conducting drone forensics: Flight data (log files), sensor parameters (GPS coordinates), root file systems, ground control techniques, station memory (internal storage), timestamps, OS, file formats, SDR board and the cognitive channels. From this study, it is evident that sensor parameters in drone forensics can allow forensic activities to be conducted as part of device-level forensics as is mentioned by [63] given that UAVs still suffer from standardization issues. Nevertheless, most of the findings broadly open the UAV area to further exploration. Research has shown that the area is currently witnessing the rise of anti-forensic techniques. In addition, drones are resource-constrained devices, and for the lesser duration that they move from the origin to the destination and back, it would be important to include an automated forensic readiness component to aid in incident planning and preparation as is articulated in [54,64–66] This is vital, as it can be used to accumulate necessary investigative data that can be used to build a forensic-rich hypothesis that can be used for a UAV investigation. Furthermore, based on a mapping of the commonalities that may exist between drone forensics and other digital forensic investigation processes, it is the author's opinion that more research on applicable standards on drone investigations needs to be explored given that the field suffers from the lack of generally accepted investigation processes at the time of writing this paper. A recent study that explored the deployment of UAVs as a dynamic approach towards enhanced policing in developing nations also highlighted this observation, albeit from a security application standpoint [2]. Thus, a standardized investigative process could present a fundamental baseline for establishing the drone forensic investigation subdomain of digital investigation. Understanding this urgency is essential in the current COVID-19 enhanced digital transcendence. Whilst the potential deployment approach of UAVs and other such related "sensor with wings" devices are being explored for diverse economic possibilities, the potential for crime increase remains an issue of concern to the forensic community.

Future works will therefore focus on implementing the proposed integrated UAV forensic model. Practical steps will be followed to observe the implementation feasibility of the model towards drone forensics, irrespective of the context. Arguably, the internal structure of diverse drones could vary from one type to another. However, within the context of a generic UAV investigation model, the abstract representation of extraction, and analysis would remain the same irrespective of the type and make of the UAV. This could, nonetheless, further introduce the need for an extraction and analysis model which are specific to a certain type of UAVs. Techniques that can be leveraged for investigating wireless communication are potential components that will be explored. Such an approach could utilize signal processing techniques, band channel analysis, as well as spectral analysis. This idea is particularly essential when developing the pre-incident preparatory phase defined in the proposed DRF model. As outlined in the proposed model, this information can be used to develop a formative baseline during the investigation phases. This can include answers to questions such as what and how to identify UAV-specific RF emission, how to distinguish UAV RF emission, as well as how to extract such RF signals.

8. Conclusions

Drone forensics has gained tremendous attention from researchers working in this field. Several frameworks and techniques have been developed, providing a deep insight into the drone application to forensic analysis. These techniques use the internal logs of devices and their controller to identify any malicious activity. They can reproduce the flight trajectories that can be used by analysts during forensic analyses. The authentication and security of drones have been also enhanced to prevent intrusion. Similarly, the communications between drones, drones to ground and ground to drone have been also improved. However, there are still challenges in the digital forensic analysis regarding UAVs. Even though there are highly secure communication channels, they have their limitation when they are applied to any IoT environment. To retrieve data from drones, digital forensic techniques are not enough for investigations. With advanced drone models hitting the market, digital forensic software/tools and techniques must undergo extensive upgrades. A comprehensive review of the existing drone forensics framework and models have been presented in this manuscript. Furthermore, an integrated forensic model was developed to provide a generic baseline for investigating a drone-related incident. The proposed model integrates components of proactive and reactive procedures towards an effective investigation. This proposition can provide a baseline towards the development of a standardized forensic investigation approach in DRF. Furthermore, the proposed investigation model can be used to achieve a digital forensic readiness system, which can be used to develop a proactive mechanism for DRFs.

Author Contributions: Conceptualization, A.A.-D., R.A.I., V.R.K., F.M.G. and S.R.; methodology, A.A.-D., R.A.I., V.R.K.; validation, A.A.-D., R.A.I., V.R.K. and F.M.G.; formal analysis, A.A.-D., R.A.I., V.R.K., F.M.G.; investigation, A.A.-D., R.A.I., V.R.K., F.M.G.; resources, A.A.-D., R.A.I., V.R.K., F.M.G.; writing—original draft preparation, A.A.-D., R.A.I., V.R.K., F.M.G.; writing—review and editing, A.A.-D., R.A.I., V.R.K., F.M.G.; supervision, A.A.-D., R.A.I., V.R.K., F.M.G. All authors have read and agreed to the published version of the manuscript.

Funding: Research supported by IOAP participant-Luleå University of Technology, Sweden.

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

References

1. Horsman, G. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digit. Investig.* **2016**, *16*, 1–11. [CrossRef]
2. 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.
3. Molnar, A.; Parsons, C. Unmanned Aerial Vehicles (UAVs) and Law Enforcement in Australia and Canada: Governance Through 'Privacy'in an Era of Counter-Law? In *National Security, Surveillance and Terror*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 225–247.
4. Philomin, S.; Singh, A.; Ikuesan, A.; Venter, H. Digital forensic readiness framework for smart homes. In Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020, Norfolk, VA, USA, 12–13 March 2020.
5. Zhang, X.; Choo, K.-K.R.; Beebe, N.L. How do I share my IoT forensic experience with the broader community? An automated knowledge sharing IoT forensic platform. *IEEE Internet Things J.* **2019**, *6*, 6850–6861. [CrossRef]
6. Kebande, V.R.; Ray, I. A generic digital forensic investigation framework for Internet of Things (IoT). In Proceedings of the IEEE 4th International Conference Future Internet Things and Cloud, FiCloud, Vienna, Austria, 22–24 August 2016; pp. 356–362.

7. Kebande, V.R.; Venter, H.S. Novel digital forensic readiness technique in the cloud environment. *Aust. J. Forensic Sci.* **2018**, *50*, 552–591. [CrossRef]
8. 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.
9. Iamsumang, C.; Mosleh, A.; Modarres, M. Monitoring and learning algorithms for dynamic hybrid Bayesian network in on-line system health management applications. *Reliab. Eng. Syst. Saf.* **2018**, *178*, 118–129. [CrossRef]
10. Lepine, M.D. Design of a Personal Aerial Vehicle. Bachelor's Thesis, Worcester Polytechnic Institute, Worcester, MA, USA, April 2017.
11. Lee, C.S.; Chan, W.L.; Hsiao, F.B. The development of Spoonbill UAV and LPV modeling of longitudinal dynamics. In Proceedings of the 23rd Bristol International UAV Systems Conference, Bristol, UK, 7–9 April 2008.
12. Al-Dhaqm, A.; Razak, S.A.; Othman, S.H.; Aldolah, A.A. Database forensic investigation process models: A review. *IEEE Access* **2020**, *8*, 48477–48490. [CrossRef]
13. Al-Dhaqm, A.; Razak, S.A.; Ikuesan, R.A.; Kebande, V.R.; Siddique, K. A Review of Mobile Forensic Investigation Process Models. *IEEE Access* **2020**, *8*, 173359–173375. [CrossRef]
14. Al-Dhaqm, A.; Razak, S.; Siddique, K.; Ikuesan, R.A.; Kebande, V.R. Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. *IEEE Access* **2020**, *8*, 145018–145032. [CrossRef]
15. Barton, T.E.A.; Azhar, M.A.H.B. Open source forensics for a multi-platform drone system. In Proceedings of the International Conference on Digital Forensics and Cyber Crime, Prague, Czech Republic, 9–11 October 2017; pp. 83–96.
16. Maarse, M.; Sangers, L.; van Ginkel, J.; Pouw, M. Digital forensics on a DJI Phantom 2 Vision+ UAV. *Univ. Amst.* **2016**, *1*, 22.
17. 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.
18. Mohan, M. *Cybersecurity in Drones*; Utica College: Utica, NY, USA, 2016.
19. Jain, U.; Rogers, M.; Matson, E.T. Drone forensic framework: Sensor and data identification and verification. In Proceedings of the 2017 IEEE Sensors Applications Symposium (SAS), Glassboro, NJ, USA, 13–15 March 2017; pp. 1–6.
20. Clark, D.R.; Meffert, C.; Baggili, I.; Breitinger, F. DROP (DRone open source parser) your drone: Forensic analysis of the DJI phantom III. In Proceedings of the DFRWS 2017 USA—Proceedings 17th Annual DFRWS USA, Austin, TX, USA, 6–9 August 2017; Volume 22, pp. S3–S14.
21. 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]
22. Llewellyn, M. *DJI Phantom 3-Drone Forensic Data Exploration*; Edith Cowan University: Perth, Australia, 2017.
23. 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.
24. Barton, T.E.A.; Azhar, M.A.H.B. Forensic analysis of popular UAV systems. In Proceedings of the 7th International Conference Emerging Security Technologies EST 2017, Canterbury, UK, 6–9 September 2017; pp. 91–96.
25. Bouafif, H.; Kamoun, F.; Iqbal, F.; Marrington, A. Drone Forensics: Challenges and New Insights. In Proceedings of the 9th IFIP International Conference on New Technologies, Mobility & Security, Paris, France, 26–28 February 2018; Volume 2018, pp. 1–6.
26. 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, 27–30 August 2018; pp. 48–52.
27. Gülataş, İ.; Baktır, S. Unmanned aerial vehicle digital forensic investigation framework. *J. Nav. Sci. Eng.* **2018**, *14*, 32–53.
28. 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.
29. 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]
30. 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]
31. 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, Tangier, Morocco, 24–28 June 2019; pp. 704–710.
32. Esteves, J.L. Electromagnetic Watermarking: Exploiting IEMI effects for forensic tracking of UAVs. In Proceedings of the International Symposium on Electromagnetic Compatibility—EMC EUROPE, Barcelona, Spain, 2–6 September 2019; pp. 1144–1149.
33. Mei, N. An Approach to Unmanned Aircraft Systems Forensics Framework—ProQuest. Ph.D. Thesis, Capitol Technology University, Laurel, MD, USA, April 2019.

34. Sciancalepore, S.; Ibrahim, O.A.; Oligeri, G.; di Pietro, R. Detecting drones status via encrypted traffic analysis. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning, Miami, FL, USA, 15–17 May 2019; pp. 67–72.
35. Le Roy, F.; Roland, C.; le Jeune, D.; Diguet, J.P. Risk assessment of SDR-based attacks with UAVs. In Proceedings of the International Symposium on Wireless Communication Systems, Oulu, Finland, 27–30 August 2019; Volume 2019, pp. 222–226.
36. Maune, K.G. A Project Completed as Part of the Requirements for BSc (Hons) Computer Forensic Investigation. 2018. Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1025.4878&rep=rep1&type=pdf (accessed on 3 March 2021).
37. Kovar, D.; Dominguez, G.; Murphy, C. UAV (aka drone) Forensics. Presented at the SANS DFIR Summit, Austin, TX, USA, 23–24 June 2016.
38. Procházka, T. Capturing, Visualizing, and Analyzing Data from Drones. Bachelor's Thesis, Charles University, Prague, Czech Republic, 2016.
39. 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.
40. 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.
41. 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, 15–17 April; 2019. [CrossRef]
42. Shi, X.; Yang, C.; Xie, W.; Liang, C.; Shi, Z.; Chen, J. Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Commun. Mag.* **2018**, *56*, 68–74. [CrossRef]
43. Guvenc, I.; Koohifar, F.; Singh, S.; Sichitiu, M.L.; Matolak, D. Detection, tracking, and interdiction for amateur drones. *IEEE Commun. Mag.* **2018**, *56*, 75–81. [CrossRef]
44. Ding, G.; Wu, Q.; Zhang, L.; Lin, Y.; Tsiftsis, T.A.; Yao, Y.-D. An amateur drone surveillance system based on the cognitive Internet of Things. *IEEE Commun. Mag.* **2018**, *56*, 29–35. [CrossRef]
45. Yihunie, F.L.; Singh, A.K.; Bhatia, S. Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles. *Smart Innov. Syst. Technol.* **2020**, *141*, 701–710.
46. Jain, U. A Drone Forensics Investigation Framework. Master's Thesis, Purdue University, West Lafayette, IN, USA, 2017.
47. Makura, S.M.; Venter, H.S.; Ikuesan, R.A.; Kebande, V.R.; Karie, N.M. Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020, Doha, Qatar, 2–5 February 2020; pp. 200–205.
48. Kebande, V.R.; Karie, N.M.; Venter, H.S. Adding Digital Forensic Readiness as a security component to the IoT domain. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1–11. [CrossRef]
49. Munkhondya, H.; Ikuesan, A.; Venter, H. Digital forensic readiness approach for potential evidence preservation in software-defined networks. In Proceedings of the 14th International Conference on Cyber Warfare and Security, ICCWS 2019, Stellenbosch, South Africa, 28 February–1 March 2019; pp. 268–276.
50. Lagrasse, M.; Singh, A.; Munkhondya, H.; Ikuesan, A.; Venter, H. Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism. In Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020, Norfolk, VA, USA, 12–13 March 2020; pp. 296–305.
51. 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.
52. Al-Dhaqm, A.; Razak, S.A.; Othman, S.H.; Nagdi, A.; Ali, A. A generic database forensic investigation process model. *J. Teknol.* **2016**, *78*, 6–11. [CrossRef]
53. Kebande, V.; Venter, H. Towards a model for characterizing potential digital evidence in the cloud environment during digital forensic readiness process. In Proceedings of the International Conference on Cloud Security Management, ICCSM, Tacoma, DC, USA, 22–23 October 2015; Volume 2015.
54. Kebande, V.R.; Venter, H.S. On digital forensic readiness in the cloud using a distributed agent-based solution: Issues and challenges. *Aust. J. Forensic Sci.* **2018**, *50*, 209–238. [CrossRef]
55. Cheng, Z.; Sun, L.; Liu, F.; Liu, X.; Li, L.; Li, Q.; Hu, R. Engineering design of an active–passive combined thermal control technology for an aerial optoelectronic platform. *Sensors* **2019**, *19*, 5241. [CrossRef] [PubMed]
56. Rodin, C.D.; Andrade, F.A.d.; Hovenburg, A.R.; Johansen, T.A. A Survey of Practical Design Considerations of Optical Imaging Stabilization Systems for Small Unmanned Aerial Systems. *Sensors* **2019**, *19*, 4800. [CrossRef] [PubMed]
57. Kebande, V.R.; Ikuesan, R.A.; Karie, N.M.; Alawadi, S.; Choo, K.-K.R.; Al-Dhaqm, A. Quantifying the need for Supervised Machine Learning in Conducting Live Forensic Analysis of Emergent Configurations (ECO) in IoT Environments. *Forensic Sci. Int. Rep.* **2020**, *2*, 100122. [CrossRef]
58. Karie, N.M.; Kebande, V.R. Building ontologies for digital forensic terminologies. *Int. J. Cyber-Secur. Digit. Forensics* **2016**, *5*, 75–83. [CrossRef]
59. Singh, A.; Venter, H.S.H.S.; Ikuesan, A.R.A.R. Windows registry harnesser for incident response and digital forensic analysis. *Aust. J. Forensic Sci.* **2018**, 1–17. [CrossRef]
60. Zawali, B.; Ikuesan, R.A.; Kebande, V.R.; Furnell, S.; A-Dhaqm, A. Realising a Push Button Modality for Video-Based Forensics. *Infrastructures* **2021**, *6*, 54. [CrossRef]

61. Omeleze, S.; Venter, H.S. Digital forensic application requirements specification process. *Aust. J. Forensic Sci.* **2019**, *51*, 371–394. [CrossRef]
62. Kebande, V.R.; Mudau, P.; Ikuesan, R.A.; Venter, H.S.; Choo, K.-K.R. Holistic Digital Forensic Readiness Framework for IoT-Enabled Organizations. *Forensic Sci. Int. Rep.* **2020**, *2*, 100117. [CrossRef]
63. Munkhondya, H.; Ikuesan, A.R.; Venter, H.S. A case for a dynamic approach to digital forensic readiness in an SDN platform. In Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020, Norfolk, VA, USA, 12–13 March 2020; pp. 584–593.
64. Karie, N.M.; Kebande, V.R.; Venter, H.S.; Choo, K.K.R. On the importance of standardising the process of generating digital forensic reports. *Forensic Sci. Int. Rep.* **2019**, *1*, 100008. [CrossRef]
65. Kebande, V.R.; Karie, N.M.; Ikuesan, R.A.; Venter, H.S. Ontology-driven perspective of CFRaaS. *Wiley Interdiscip. Rev. Forensic Sci.* **2020**, *2*. [CrossRef]
66. Singh, A.; Ikuesan, A.; Venter, H. A context-aware trigger mechanism for ransomware forensics. In Proceedings of the 14th International Conference on Cyber Warfare and Security, ICCWS 2019, Stellenbosch, South Africa, 28 February–1 March 2019; pp. 629–638.