Digital Forensic Investigation of an Unmanned Aerial Vehicle (UAV): A Technical Case Study of a DJI Phantom III Professional Drone

Robinson Tombari Sibe[1,*], David Bekom[2]

[1]Rivers State University, Nigeria/ Digital Footprints Ltd, Nigeria
[2]Digital Footprints Ltd, Nigeria
Emails: robinson.sibe@ust.edu.ng; david.bekom@digitalfootprints.ng

Abstract

Globally, drones have become increasingly popular. While there are legitimate uses of drones, there are also complaints of increasing deployment for illegal activities. With the increasing caseloads of unethical, illegal, and criminal deployments, investigators have become more interested in conducting forensic examination of drones, to reconstruct events and provide answers to key investigative questions. This technical case study is a digital forensic investigation of a DJI Phantom III Professional drone to obtain possible evidential artifacts. The paper outlines the procedures and tools that were employed to acquire, preserve, analyse, and present digital evidence from the drone and its associated accessories. The paper also discussed the current state of the body of knowledge and the challenges in the field of drone forensics. An outcome of this study was the development of a drone forensic investigation model, inspired by the DFRWS Framework. The result of this investigation produced valuable evidential artifacts deconstructing vital flight information and other parameters of the drone, obtained in a forensically sound and legally defensible manner.

Keywords: Drone forensics; drone investigation; digital forensics; UAV investigation; digital investigation; mobile forensics; cyber forensics; cybersecurity

1. Introduction

With the advancement of technology and the proliferation of viable applications, Unmanned Aerial Vehicles (UAVs), commonly known as drones, have become ubiquitous in various domains, such as media, commerce, security, and military. However, the widespread use of drones also introduces new challenges and threats to the security and privacy of individuals, organizations, and society, as drones can be compromised, manipulated, or exploited by adversaries for malicious purposes [6], [9]. Hence, there is a growing need and demand for digital forensic investigation of drones, which is a specialized branch of digital forensics that deals with the acquisition, preservation, analysis, and presentation of digital evidence from drones and their related devices, such as remote controllers, storage media, cameras, and sensors. This paper reviews the current state of knowledge and techniques for conducting digital forensic investigation of drones, such as identifying the drone model and manufacturer, extracting, and decoding the data stored on the drone, the possibility of recovering deleted or encrypted data, locating the drone operator and the flight path, and correlating the data from different sources.

The existing research works on the subject were reviewed and the future research directions and gaps in this field were identified. Forensic analysis of a real UAV acquired after regular field usage in real-life application is carried out to obtain evidential artifacts which can be of use in determining the specifics of an event involving the UAV. Multiple commercially available and free tools were used to decode and interpret the data obtained from the storage media.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

This paper was structured in the following order: The Literature Review section provides an overview of the current state of drone forensics, covering the main challenges, methods, tools, and standards in this domain. Previous efforts were highlighted as well. The materials and Methods section described the process design utilized as well as tools and measures undertaken to maintain forensic soundness. In Results and Findings, the obtained results and their importance were discussed. In the final section, Conclusions were stated and recommendations for future work in the field are put forward.

A. Problem Statement

Drones have become increasingly popular, with a wide range of applications in different sectors and endeavors. While there are lots of legitimate uses of drones, there is also a growing use in criminal domains. With increasing deployments for both categories of users, expectedly, there are more drone incidents – routine aviation audits, drone accident, and criminal activities – needing drone forensics in the investigation process [6], [9].

Over the years, there have been several research efforts in the field of drone forensics. However, despite these commendable efforts, there is an obvious gap in terms of robust drone forensic studies out there. Most of the available peer-reviewed drone forensic studies have been limited by the range of forensic toolkit available to researchers. That is, the studies were constrained to one or just a few tools and limited by the limitations of that tool. Therefore, this study addresses this gap by using a robust range of digital forensic toolkit, consisting of some of the most widely used and respected forensic tools – both commercial and open source. The use of different tools for one investigation avails the researcher the opportunity for correlation and cross-validation of findings, which is critical for integrity and reliability.

Beyond the challenge of lack of sufficient research efforts in drone forensics, there is also the general challenge of the complexity of extraction, preservation, and analysis of digital evidence in a forensically sound manner, admissible in courts or special panels of investigation. This challenge is even more pronounced with drone forensics, given the unique complexities of drones. To further complicate things, there is the challenge of the lack of proprietary technical documentations by drone manufacturers. This is perhaps a deliberate privacy-by-design strategy by manufacturers, as an anti-forensic tactics to protect privacy and confidentiality of drone users and data acquired.

Finally, there is also the challenge of lack of standardisation of the drone forensic investigation process. From a general digital forensic perspective, drone forensics is broadly classified and approached as mobile forensics. However, drones are uniquely complex, and technically different from mobile phones. This paper addresses this problem by evolving a drone forensic investigation model, with specific reference to processes, evidential artifacts recovered, and the tools used. This is a unique contribution of this study and adds to the growing drone forensic research output.

2. Literature Review

A. The Increasing Adoption of Drones

Drones have become increasingly popular in recent years. With the increasing applications in different fields, there have been a rapid proliferation in use of drones [5]. For instance, the Federal Aviation Administration [19] puts the total number of drones registered in the United States of America at 790,918. Out of this number, 369,528 were drones registered for commercial purpose, 416,095 were registered for recreational purpose, and 5,295 paper registrations. The global drone market size was valued at $43 billion in 2022 by Drone Survey Services [13]. Statista (2023) estimated the global drone market revenue at $4 billion in 2023. From an industry and sectoral perspective, the agriculture sector is the largest market for commercial drones. The global agriculture drone industry is estimated at $380 million in 2023 [13].

Drones have become increasingly popular due to its wide applicability, beyond the traditional application in the military and law enforcement. Today, there are several applications of drone in both the military and commercial space. For instance, drones have revolutionalised supply chain logistics, particularly in difficult terrains. Quite disturbingly, while most of the drone applications are ethical, there are growing concerns for the unethical and criminal use of drones [4], [9]. The rise in cybercrime activities involving drones have led to a growing interest in digital forensic investigations of drones. Due to several challenges, including the choice of tools, the process of collecting digital evidence from drones that have been seized, and establishing a case in court, has been quite challenging. To guarantee accuracy in reporting, it is best practice to ensure that the forensic investigation tools used in an investigation must have been tested and validated before being used [33]. Therefore, in collecting and analyzing drone artifacts, this must be done in a forensically sound and legally defensible manner.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

B. Drone Features

A drone is a type of unmanned aerial vehicle (UAV) that can fly autonomously or remotely controlled by an operator. According to their lifting power, drones can be classified into two categories: heavier-than-air (HTA) and lighter-than-air (LTA) [2]. HTA drones include fixed-wing, rotary-wing, and hybrid drones that rely on aerodynamic forces to generate lift. LTA drones include airships or blimps that use buoyant gas to float in the air. HTA drones are more suitable for high-speed and long-range missions, while LTA drones are more suitable for low-speed and long-duration missions [26].

The technical components of a drone vary depending on its type, size, and function, but generally include a frame, a propulsion system, a control system, a communication system, a navigation system, a payload system, and a power system. The frame provides the structure and support for the drone and its components. The propulsion system consists of motors, propellers, and speed controllers that enable the drone to move and maneuver in the air. The control system includes sensors, actuators, and controllers that regulate the drone's attitude, altitude, and position. The communication system enables the transmission and reception of data and commands between the drone and the ground station or other drones. The navigation system includes global positioning system (GPS), Inertial Measurement Unit (IMU), compass, barometer, and other sensors that provide information about the drone's location and orientation. The payload system consists of cameras, sensors, or other devices that enable the drone to perform its specific task or mission. The power system includes batteries or fuel cells that provide energy for the drone's operation [8]. The Inertial Measurement Unit (IMU) is a device that measures the orientation, angular velocity, and linear acceleration of an object by using a combination of sensors such as gyroscopes, accelerometers, and magnetometers [34].

For surveillance purposes, drones can be equipped with various types of cameras or sensors that can capture images or videos of the target area or object. For example, drones can use optical cameras for daytime surveillance, infrared cameras for nighttime surveillance, thermal cameras for heat detection, multispectral cameras for vegetation analysis, and hyperspectral cameras for material identification, lidar sensors for distance measurement, radar sensors for obstacle detection, or acoustic sensors for sound detection. Depending on the scenario, drones can use different modes of surveillance, such as stationary surveillance, where the drone hovers over a fixed point; patrolling surveillance, where the drone follows a predefined route; tracking surveillance, where the drone follows a moving target; or cooperative surveillance, where multiple drones work together to cover a larger area or provide different perspectives [8].

Drones can store an extensive amount of evidence that could be crucial to drone incident investigations. This comprises the drone's flight path, flight date and time, altitude, home point, and warnings indicating whether the drone is approaching restricted airspace such as airports (No Fly Zones). Furthermore, it was discovered that while manufacturers can incorporate Anti-Forensics software into their gadgets, the regular drone users may not have the capabilities to use such complex techniques [7].

C. Legal Framework for Operation of UAVs

In response to the significant increase in the usage of UAVs for civilian purposes, the European Union (EU) adopted a common regulatory framework to ensure safe, secure, and sustainable drone operations across its member states. The framework consists of two main regulations: Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of UAS, and Commission Implementing Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft [16]. These regulations establish three categories of drone operations based on the level of risk involved: open, specific, and certified. The open category covers low-risk operations that do not require prior authorization or declaration by the drone operator. The specific category covers medium-risk operations that require authorization by the national aviation authority or compliance with a standard scenario. The certified category covers high-risk operations that require certification of the drone, the operator, and the remote pilot, as well as compliance with aviation rules [17]. The regulations also set out technical and operational requirements for drones, such as registration, identification, geo-awareness, remote control, insurance, and data protection. The EU drone regulations aim to harmonize the legal framework for drone operations within the EU, foster innovation, and competitiveness in the drone sector, and protect the safety, security, and privacy of citizens and the environment [18].

Drone operators also need to comply with the EU's General Data Protection Regulation (GDPR) when they collect personal data by taking measures such as informing the data subjects, obtaining their consent, anonymizing the data, respecting their rights, limiting the purpose and duration of data use, protecting the data from unauthorized access or transfer, and assessing the potential risks of data processing. Failure to comply with the GDPR may result in fines and penalties for drone operators [12]. Thus, the GDPR is an important factor to consider when storing data on drones.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

In Nigeria, the Nigeria Civil Aviation Authority (NCAA), is the agency responsible for Aviation safety in Nigeria. The NCAA is saddled with the responsibility of regulating the use of drones in Nigeria. The Nigeria Civil Aviation Authority guidelines for unmanned Aircraft System Operations in Nigeria provides that all UAV operators must obtain a Remotely Piloted Aircraft Systems Certificate (RPAS) before flying in Nigeria and register their drones if they weigh more than 250 grams or have a camera [28]. The RPAS certificate requires the operators to submit a flight plan to the NCAA for approval before conducting any drone flight within Nigeria and to comply with the guidelines for the operations of remotely piloted aircraft systems/unmanned aerial vehicles (RPAS/UAV) in Nigeria. There are not many technical requirements for UAVs outlined by the NCAA.

D. Related Works

Although drones have become increasingly popular, there are not many robust research and literature on the subject. However, in recent years, some researchers have made significant progress in studies involving the extraction and analysis of digital artifacts found in UAVs, and in effect contribute to the body of knowledge. Some of the most notable are presented in this section.

Clark et al [11] investigated how to extract forensic evidence from a DJI Phantom III drone, a popular type of drone that has been involved in both legal and illegal operations. The paper described how to analyze the drone's hardware and software components, as well as the smartphone that controls it, and how to decode the data they store, such as location, flight, battery, camera, and device information. The paper also introduced a new tool called DROP (DRone Open-Source Parser) that can help forensic examiners parse the data from the drone. The researchers acknowledge the difficulties and risks of performing forensic analysis on drones, such as the physical disassembly, the lack of official documentation, and the legal and ethical implications of drone privacy and security. This work builds on previous research work by applying different tools and methods (open-source and commercial).

Bouafif et al. [9] carried out forensic analysis on a Parrot AR drone 2.0 in which the research provided several insights into the field, including methods of attributing ownership of a UAV device by examining associated controller Android IDs and accessing the file system of the device using FTP or Serial connections. Using the stated methodology, the researchers were also able to obtain flight path data from the UAV along with media files captured with the attached camera. Viswanathan et al. [33] shared their research on the intelligent sorting of DJI Mavic Air drone data and tool selection. Using sample drone data from the Computer Forensic Reference Dataset (CFReDS) project, the researchers analyzed the UAV flight logs with tools such as Airdata, Autopsy, and CsvView. The proposed approach is useful to forensic investigators in determining the most relevant forensic investigation instruments.

Iqbal et al. [23] carried out a drone forensic investigation, with the aim of reconstructing drone events using forensically acquired artifacts from the drone. The study investigated if the drone was vulnerable to attacks. Specifically, the study forensically investigated a Parrot Bebop 2 drone and the drone controller, an iPhone 6S phone. Flight data, recorded media by the drone, and ownership information were extracted and analyzed using FTP and iTunes backup. A major outcome of this study was to show that the Parrot Bebop 2 drone had vulnerabilities that could be exploited, as well as establishing ownership, and reconstructing drone events.

A comprehensive forensic analysis of two popular UAV models: DJI Phantom 4 and DJI Matrice 210, which have been involved in several cases of illegal activities was carried out by Salamh et al. [30]. The study evaluated the performance of three forensic software tools (Autopsy, Magnet AXIOM, and Cellebrite) for extracting and analyzing digital evidence from UAVs, such as flight logs, media files, and GPS data. The paper also proposed a three-dimensional visualization technique for presenting the flight paths recovered from UAVs, which can help forensic examiners reconstruct events and scenarios. Furthermore, the researchers presented the challenges and limitations of decrypting and verifying the flight logs from UAVs and suggested possible solutions to enhance the integrity and reliability of the forensic evidence.

3. Methodology

This forensic case study is based on a DJI Phantom III Professional drone. With an estimated global market share of 54% in 2022 (and 80% market share in the US), DJI is the largest consumer drone manufacturer in the world [13]. The DJI Phantom III Professional is a quadcopter drone that features a high-definition camera with a 3-axis gimbal for image stabilization. The drone features a propulsion system that enables a maximum flight speed of 16 m/s and a maximum flight time of 23 minutes. The drone also has a vision positioning system that allows it to hover precisely indoors or in low-GPS environments. The drone can be controlled by a remote controller or by a smartphone or tablet with the DJI GO application. The application also provides live video streaming, intelligent flight modes, and access to advanced settings and features. Some of the intelligent flight modes include Follow Me, Point of Interest, Waypoints, Home Lock, and Course Lock. The drone also has a return-to-home function

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

that automatically brings it back to the take-off point when the battery is low or the connection is lost. The drone also has LED lights that indicate the status and direction of the device [15]. Figure 1 shows the DJI Phantom III device being forensically examined.

For the investigation carried out in this study, no accompanying devices (such as a paired smartphone or controller) were given to the research team by the drone owner. Therefore, this research focused on forensically extracting digital evidence from the DJI Phantom III drone, itself. This was a constraint in this research, as previous studies by Iqbal et al. [23] showed that valuable forensic artifacts could be extracted from the device controller.

The digital forensic investigation and analysis was carried out completely in a standard digital forensic laboratory at Digital Footprints Nigeria Limited, Abuja, Nigeria. The investigation involved identifying, isolating, examining, extracting, and analyzing the data from the UAV's internal and external storage using a combination of open-source and commercial forensic tools. The investigation followed the Standard Operating Procedure of the organisation which is in line with best practice, and consistent with the Interpol [22] framework for responding to a drone incident. Table 1 shows the various software tools used in this forensic investigation and research. Table 2 shows the hardware used for the investigation.

Figure 1. DJI Phantom III Professional drone.

The software tools listed are subject to regular validations as part of the laboratory's Standard Operating Procedure (SOP) and were confirmed up to be accurate as at date at the time of the forensic investigation. Also, the commercial and open-source tools used in this research have undergone reliability checks and gone through the National Institute of Standards and Technology (NIST) [35] Computer Forensics Tool Testing Program (CFTT). The hardware devices used in this investigation is shown in Table 2 below.

Over the years, to achieve standardization, different researchers have come up with several digital forensic investigative frameworks and models. For instance, Pollitt [29] proposed the 4-step process modelled after the regular court process for the admissibility of physical evidence. The steps are acquisition, identification, evaluation, and admission. Carrier and Spafford [10] also introduced the Integrated Digital Investigation Model, also patterned after the physical investigation process. This model consisted of 17 phases that were grouped into 5 phases, namely: Readiness Phases, Deployment Phases, Physical Crime Scene Investigation Phases, and Review Phase. Carrier and Spafford [10] would later modify this to reflect digital investigation, more than physical investigation [1]. This was modified and simplified to the following five primary phases: Readiness Phase, Deployment Phase, Physical Crime Investigation Phase, Digital Crime Scene Investigation Phase, and the Presentation Phase.

There are many other investigative models, but this research developed an investigative model adapted from a framework proposed by Carrier [14]. The DFRWS Framework is a 6-step investigative approach, consisting of the following steps: Identification, Preservation, Collection, Examination, Analysis, and Presentation. Over the years, because of the standardized nature of this framework, it has received wide popularity, and has attracted the attention of researchers seeking to improve on it [32]. It is also for this reason that this research adapted the DFRWS Framework, with specific modifications and implementation to suit the forensic case study.

The research methodology adopts a 4-step approach, listed in Table 3, and mapped against the corresponding DFRWS [14] steps – Identification and Preservation, Acquisition, Examination/Analysis, and Results. The hardware devices used in this investigation is shown in Table 2 below. The investigative model developed and used for this research is shown in figure 2.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

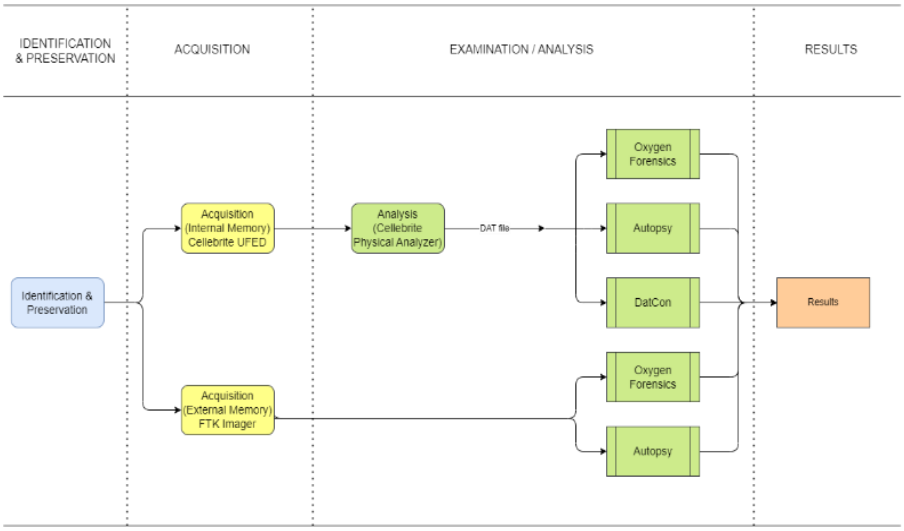

Figure 2. Drone Forensic Investigation Model developed for this study.

As illustrated in Figure 2, the model developed for this study is detailed as:

1. Identification & Preservation:

Identification and preservation the UAV device. This is important to avoid evidence contamination, so that the results of the investigation will be forensically sound and legally defensible.

2. Acquisition:

Acquisition of the internal device storage using Cellebrite UFED.

Acquisition of a forensic image of the external SD Card using FTK imager.

3. Examination/Analysis:

Analysis of the obtained .ufd file using Cellebrite Physical Analyser and exporting the raw DAT files.

Analysis of the file structure and contents of the DAT file.

Analysis of the DAT files using Oxygen forensic Detective, Autopsy and DatCon to obtain flight data.

Analysis of SD Card E01 image with Oxygen forensic detective and Autopsy.

4. Results:

Documentation and reporting of findings.

Table 1: Software Tools Used

Tool	**Software version**	**Availability**
Autopsy	4.21.0	Open source
Cellebrite Physical Analyser	7.63.0	Commercial
Cellebrite UFED 4 PC	7.65.0.247	Commercial
DatCon	4.3.0	Freeware
FTK Imager	4.7.1	Freeware
HxD Hex Editor	2.5.0.0	Freeware
Oxygen Forensic Detective	16.1.0.172	Commercial
Sigcheck	2.90.0.0	Freeware

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

A. Identification and Preservation

An important first step is the identification of the evidence item. In this case, the drone which serves as the forensic case study was willfully handed over to the researchers by the drone owner, with relevant chain of custody and authorization documentations signed in line with industry best practice. Also, in line with digital forensic best practice, the physical appearance and condition of the drone and its components were documented before any further contact with the device. Figure 3 shows the identifiers on the exterior of the drone. One of the steps taken to ensure the validity and integrity of the obtained data was to maintain the chain of custody of the data collected. This accounts for evidence at every stage of the investigation and shows that the device and data were handled and stored in a secure and documented manner, preventing any unauthorized access or tampering. Maintaining the chain of custody is important for preserving the integrity and reliability of the data, as well as for complying with ethical and legal standards [20].

In digital forensics, it is best practice to get a forensic copy of an evidence item, so the analysis can be done on the copy and not the original. To get a forensic copy and ensure the integrity of the device, a write blocker was used in the forensic duplication process [25]. In this research, a write block enabled card reader was used to create a bit-by-bit copy of the external storage media on the drone. This prevented any modification of the original data and provided a verifiable hash value for authentication. Also, in line with industry best practice, the drone was left powered off during acquisition to prevent writing to the non-volatile storage of the device leading to evidence contamination.

Figure 3. Device identifiers on the drone.

Table 2: Hardware Tools Used

Equipment	**Operating System/Firmware**
Digital Intelligence F.R.E.D Workstation	Microsoft Windows 10
Cellebrite UFED Device Adapter	n/a
Cellebrite Card Reader	n/a

B. Data Acquisition

This research used the mobile forensic tool, Cellebrite Universal Forensic Extraction Device (UFED), for data acquisition from the drone. Cellebrite UFED is a commercial mobile forensic tool recognized globally as one of the top mobile forensic tools [24], [21]. Also, Cellebrite UFED has undergone reliability checks by the National Institute of Standards and Technology (NIST) [35] Computer Forensics Tool Testing Program (CFTT). Also, in line with Quality Control protocols of Digital Footprints Laboratory, all forensic tools are subjected to quarterly tool validation protocol. The last tool validation for the laboratory was done 26 days before the commencement of this research.

The internal storage of the drone was acquired using Cellebrite UFED, which allows for the extraction of data without modifying the original source. This method was chosen over simply connecting the device to a computer and copying the files (which would work for this model of DJI UAVs but not on some others), as the latter could alter the metadata or introduce artifacts that would compromise the integrity of the evidence. The drone was kept powered off until the extraction process was initiated, to prevent any potential data loss or evidence contamination.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

Forensic analysis of UAVs in highly sensitive cases may require the extraction of flight data without altering the original evidence. Turning on the UAV may cause new data to be written to its internal storage, which could affect the forensic soundness and admissibility of the investigation. One example of such a situation is where the storage capacity of the device is exhausted and to store new flight data logs, existing ones would have to be rolled over. Therefore, a possible solution is to disassemble the UAV and access the internal SD card that stores the flight data. The SD card is usually attached to the main board of the UAV and can be removed with appropriate tools and skills. By doing so, the analyst can obtain a physical copy of the flight data without modifying the original data on the UAV.

The 64-gigabyte external SD card was carefully removed from the device and connected to the forensic workstation using a Cellebrite USB SD card reader with hardware write blocking enabled, which prevents any modification of the data on the card. The card was then imaged in E01 format using FTK Imager, a forensic software that can create bit-by-bit copies of digital media.

Table 3: Drone Forensic Investigation Method Used

Drone Forensic Investigation Process	**DFRWS Equivalent**
Identification and Preservation	Identification and Preservation
Data Acquisition	Collection
Examination/Analysis	Examination and Analysis
Result Reporting/Presentation	Presentation

C. Data Analysis/Examination

The obtained forensic image of the device was analyzed using Cellebrite Physical Analyser which is an industry-standard software forensic tool used for analyzing forensic copies of devices obtained with Cellebrite UFED. Also, Cellebrite Physical Analyser has undergone reliability checks by the National Institute of Standards and Technology (NIST) Computer Forensics Tool Testing Program (CFTT) [35]. The only source of flight data for the case is the UAV storage as no accompanying devices were obtained. The flight data was found on the 4-gigabyte internal SD card and was stored in DAT files. Analysis of the acquired flight data suggested that for every power on/power off cycle, a new DAT file was created. In this research, Cellebrite Physical Analyser was unable to parse the DAT files on the internal storage, so the DAT files which are central to the investigation were exported to a folder on the forensic workstation to be analyzed using other tools highlighted in Table 1. The reason for which Physical Analyser was unable to decode the DAT files was unknown to the researchers, as the specific UAV model being investigated was listed among compatible models which Cellebrite can extract and analyze data from. DatCon, Oxygen Forensic Detective, and Autopsy were used to extract data from the files. Further analysis and examination also showed that the external SD card was found to have been formatted with the exFAT file system and was used to store images and video recorded by the UAV camera.

D. DAT file structure

The DAT files as implemented by DJI followed a naming system of "FLY" followed by a three-digit number and the ".DAT" file extension (for example, FLY824.DAT). There is little officially documented information about the nature and encoding of these files. However, over time, researchers and other experts have produced tools that can decode them. In this forensic investigation, the hex dump of the DAT files obtained was analyzed using a hex editor to observe any notable characteristics of the file structure. The DAT file format is mostly unreadable. Analysis showed that only the first 42 bytes of the file are in plain text which reads "BUILD Jun 19 2017 21:40:20" after the first 128 bytes, the byte sequence "55 2C 00 57 00 80" is seen and indicates the beginning of the encoded flight data.

E. Analysis with DatCon

One of the few tools found to be able to decode DAT files was DatCon, a free tool developed with Java. DatCon 4.3.0 was used to parse the file successfully. Parsing the DAT file can produce CSV, TXT, and KML files as output. The CSV file contained values from different sensors and systems onboard the UAV. Detailed descriptions of each column were on the official website of DatCon. The text file contained event logs in plaintext ASCII format. The KML files store GPS points from the flight of the drone which could be used to reconstruct the flight path and can be plotted on a mapping application such as Google Earth or ArcGIS. Figure 4 shows the GPS points from the obtained kml file overlayed on Google Earth.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

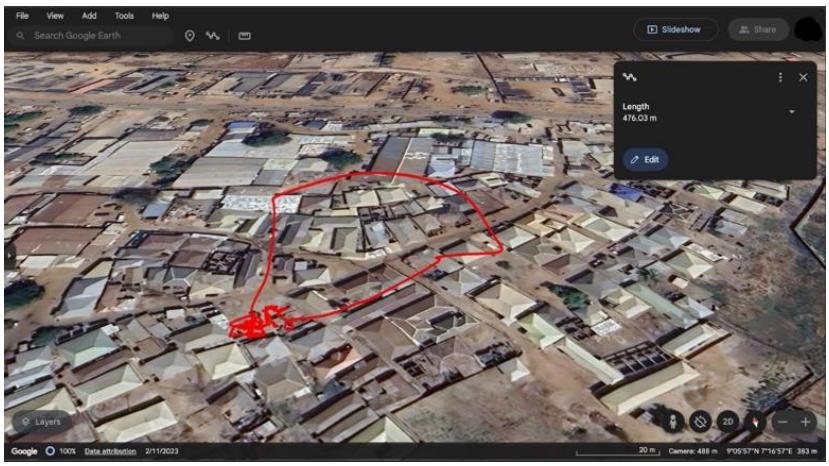

Figure 4. GPS Points from the KML file output overlayed on Google Earth.

F. Analysis with Autopsy

The data files were loaded into a newly created case in Autopsy 4.21.0. The custom ingest module "DJI Drone logs" was executed on the imported files to extract and parse the drone flight data. The module generated GPS Tracks as output artifacts, which contained the geospatial coordinates of the drone's flight path. The GPS Track artifacts were further examined and visualized on the Geolocation tab of Autopsy's interface. Figure 5 shows the artifacts on Autopsy.

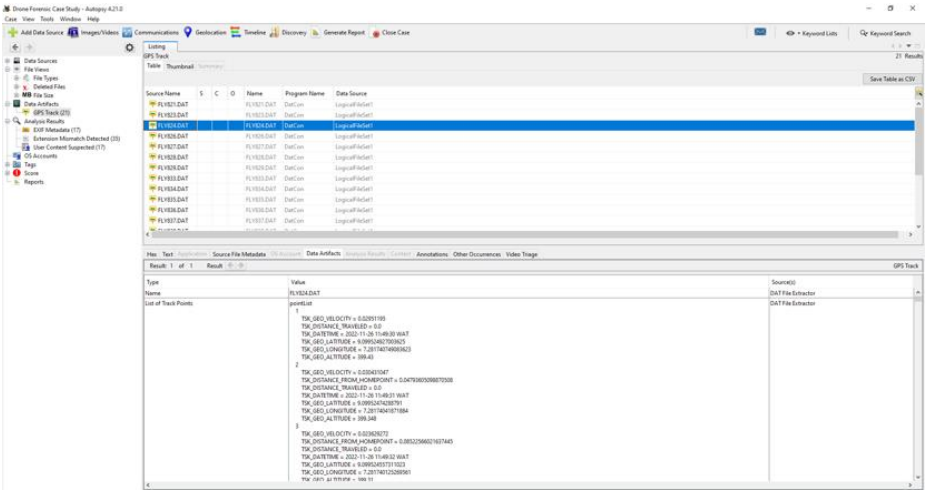

Figure 5. GPS artifacts on Autopsy.

G. Analysis with Oxygen Forensic Detective

The data files were analyzed using Oxygen Forensic Detective 16.1.0.172. The DAT files were decoded to three types of artifacts: Points, which were sensor readings sampled at a frequency of 4 Hz; Home Points, which were the coordinates of the take-off locations used for the return-to-home (RTH) function during flight; and Debug, which were system logs and debugging information. Using Oxygen Forensics, key sensor parameters such as altitude, velocity, ground speed, number of satellites, temperature, battery voltage and power were found. Figure 6 shows the sensor readings correlated to time.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

Figure 6. Plot of sensor readings correlated to time.

The flight paths were visualized using Oxygen Forensic Maps to reconstruct and analyze flight events and display the UAV sensor data at any arbitrary point along the flight path. The software also generated graphs that show the variation of Altitude, Velocity, and number of satellites in communication, Inertial Measurement Unit (IMU), and Battery health statistics as a function of time in the flight path replay. As can be seen in the flight map in figure 7 generated by Oxygen Forensics, the drone was flown in the Abuja municipal council area. Oxygen Forensics has a functionality that animates the flight path overlayed on a map. This simulates the actual flight path displayed over satellite imagery. With this, accurate display of the flight path and parameters were gotten in a forensically sound manner.

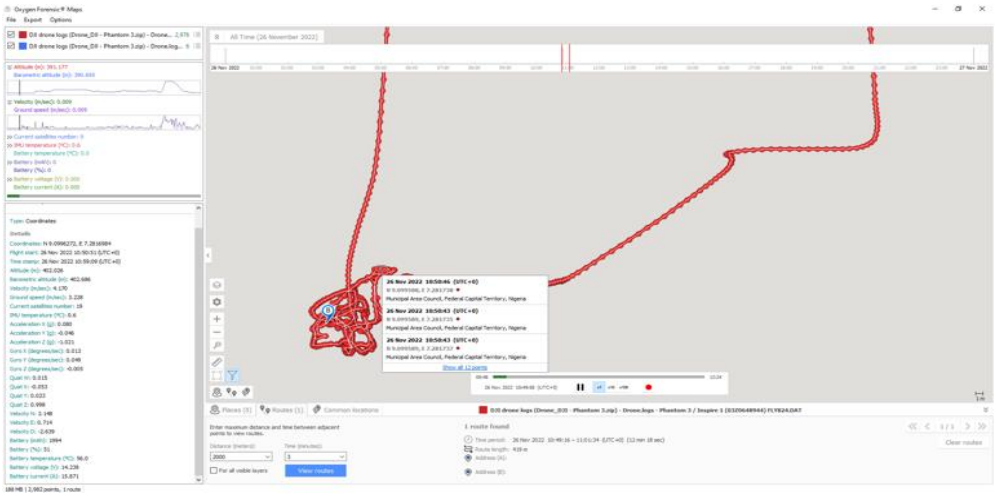

Figure 7. Flight replay view in Oxygen Forensic Detective.

H. Media Files Analysis

Autopsy and Oxygen Forensic Detective were used to analyze the forensic image of the external SD card. EXIF metadata were the primary artifacts of interest. EXIF data is an Exchangeable Image File Format file common on digital cameras. Since the drone being investigated has a camera, then EXIF data would expectedly be present in the external SD card of the drone under investigation. Several deleted image and video files of possible evidential value were recovered using file carving on Autopsy. In the “MISC” folder, information about the camera attached to the UAV was found in the “Version.txt” file. A common anti-forensic tactic is the deletion of artifacts by the suspect. Therefore, recovery of deleted EXIF data can be crucial to solving complex investigations. In this research, several image and video files that were deleted were recovered and analyzed to establish relevance to the investigation.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

4. Results/Findings

The forensic analysis of the DJI Phantom III Professional drone revealed several artifacts that were extracted from its internal and external memory. The internal memory contained DAT binaries that stored the flight and device logs, which included information such as GPS coordinates, altitude, speed, battery level, and sensor readings. These details are crucial in accurately recreating the flight activities of the drone, and other parameters of interest in a typical drone incident investigation. Figures 4-7 show key flight information forensically produced by this study. Without getting prior briefings on the drone activities, this forensic investigation correctly recreated the flight activities with scientific precision. These findings were corroborated by the drone pilot/owner.

The DAT files contained encoded data that represent the readings from the UAV's Inertial Measurement Unit (IMU). The IMU is a device that measures and reports the UAV's orientation, velocity, acceleration, and gravitational forces [3]. Autopsy, Oxygen Forensic Detective, and DatCon were the tools used in the analysis. One of the main differences among these tools (apart from the general classification if they were commercial, open source, or freeware) is the sampling rate at which they decode and display the IMU readings. Autopsy was found to have a sampling rate of 1Hz, meaning it shows one value per second. DatCon has a variable sampling rate that can be adjusted by the investigator from 1Hz to 200Hz, with a maximum limit of 2147483647Hz. Oxygen Forensic Detective has a variable sampling rate of between 4Hz and 200Hz. The sampling rate affects the granularity and accuracy of the IMU readings, as well as the size and complexity of the data set.

Using Sigcheck, a command line utility for checking file information and verifying authenticity and integrity, it was observed that the DAT files, on average had entropies of about 7.6 which would normally be indicative of either compression or Encryption [27] and the file had no compression headers. Without being decoded, the DAT file is mostly unreadable. Analysis of the Hex dumps of the acquired files showed that only the first 42 bytes of the file are in plain text which reads “BUILD Jun 19 2017 21:40:20” (It can be reasonably deduced that this may be the build time and date for the device firmware) after the first 128 bytes, the byte sequence “55 2C 00 57 00 80” is seen and indicates the beginning of the encoded flight data. The first 128 bytes can be read as the file header and can be used as an indicator to automatically identify DJI DAT binaries in a forensic tool as shown by Clark et al. [11].

The external SD card which is used by the UAV to store captured images and videos, also produced key evidential items of interest. The main source of digital evidence artifacts was the EXIF metadata of these media. Analyzing the media content also produced the pictures captured by the drone. The analyzed items had images and videos that captured the UAV’s surroundings during its operations. The EXIF metadata showed attributes consistent with the flight information recovered. Also, a close examination of the recovered EXIF data shows images consistent with the surrounding landmarks of the flight path.

In summary, the following evidential items were recovered from the SD card retrieved for the drone investigated: 40 image files, 34 audio files, 1 database file, 2 text files. The analysis of the flight data showed that the flight operated around the Abuja metropolis on the 26th of November 2022. The specific flight path was recovered and viewed in a forensically sound manner. The forensic examination and analysis showed that the drone had a travel length of 419m and total travel time of 12 minutes 18 seconds. Oxygen Forensics was used to animate the flight path, which showed the drone navigation displayed on the satellite imagery. This simulation of flight path made for excellent visualization. The outcome of this forensic research provided crucial answers to drone investigative questions such as: when, where, what, who, and if correlated with other evidential items, what. Therefore, drone forensics can be widely applied in accident/incident investigation, crime investigation, privacy investigation, and many other application areas.

5. Limitations

This study had some limitations. The lack of available documentation on the proprietary DAT file format (except for the works of a few researchers and industry experts) presented a significant hurdle to the forensic analysis. There is a possibility for even more artifacts to be obtained from the binaries with a better understanding of the data structure and algorithms used to obfuscate the data.

Evidence preservation is also an issue because the UAV must be powered on to read the contents of the internal SD card through a USB connection. This can however be overcome by disassembling the UAV and physically detaching the card which is permanently attached with an adhesive from the motherboard of the device. This procedure is delicate and complicated and the forensic examiner risks damaging the SD card or other internal components. However, due to the experience of the researchers, this was achieved without a damage.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

In this case study, analysis of only the UAV produced a critical information on its operations. Additional devices may not improve the quality of flight data obtained from the DAT files but if an accompanying smartphone is obtained with the UAV, investigators have a higher chance of attributing the actions that were performed with the drone to a specific operator. This is consistent with the findings of previous works by Iqbal et al. [23] that device controllers such as mobile phones could also produce valuable evidential artifacts of interest that could be correlated with extracted data from the drone itself. Therefore, this study was limited to only analysis of the UAV itself, and not the controller or ground station device.

6. Conclusion

This case study was done to show how much data could be obtained from the UAV in a scenario where accompanying devices were not obtained along with the device. The analysis of the log files extracted from the target system yielded varying details in terms of results (but with consistent implication) depending on the tools employed for the decoding process. The commercial tool provided a superior output in terms of clarity, completeness, and user-friendliness, while the other tools displayed the data in less optimal ways that required further interpretation or complex operations. This research correlated the findings from the different tools, and allowed for cross-validation, thereby improving the quality and reliability of the research outcome. Anti-forensics is a common issue in the field of digital forensics, no matter the device being examined. Examination of the UAV shows that the storage methods used are regular SD cards formatted with the exFAT file system. This means existing anti-forensic methods applied to SD cards can be used to prevent investigators from finding evidence artifacts on UAVs. On DJI models such as the one examined, securely deleting the DAT binaries from the internal SD card may prevent an investigator from retrieving as much information as in this case. Much progress has been made with commercial forensic tools in recent years, however, open-source tools, while capable, rarely have the capability to carry out end-to-end processing on the DAT files. This study found that most often, multiple open-source tools would be required to carry out the same amount of processing and enrichment that one of the commercial forensic tools used in this study, would handle completely.

This paper demonstrated the necessity of performing cross-validation of the outcomes derived from various analysis tools through a case study. The case study revealed that different tools can produce consistent results, but they may differ in the presentation format and the degree of detail they provide. Therefore, cross-validation is essential to ensure the reliability and validity of the analysis, as well as to identify the most suitable tool for the specific research question and data set. Importantly, this research enriched the body of knowledge in digital forensics. Key outcomes of this study include identification of research gaps, and unique contributions to fill the gap. The study established that the lack of documentation and the deliberate anti-forensic tools embedded in the design (particularly to reinforce privacy of drone users) by the manufacturer, was a key challenge in drone forensics. This study made a significant contribution by developing a model for drone forensics, as shown in figure 2, which can be adopted by researchers and practitioners. The study reinforced the need for cross-validation in the drone forensic process to improve the reliability of the research outcome. Finally, this research showed the importance of drone forensics, and the potential application in crime investigation, incident/accident investigation, and other related digital investigations. Criminals are increasingly deploying drones for criminal activities, and this research proved that drone forensics can be deployed to reconstruct drone events, acquire evidence in a forensically sound manner, and ultimately aid in the prosecution of the criminals. This research showed that drone forensics can answer key questions such as, where and when drone was used, flight path, devices paired with, pictures and videos taken, speed, altitude, battery power, and many other attributes of interest.

A. Recommendations for future research.

With the ongoing advancements in the field of Drone (UAV) forensics, there is a growing need for efforts to be made to standardize the process of carrying out investigations of UAVs. The current state of the field is largely modelled according to the mobile forensics process. It is however worth noting that Unmanned Aerial Vehicles vary significantly from mobile phones and while there exist several artifacts of note on accompanying mobile phones, the UAV is a separate device and as such, needs its own standardized procedure for forensic investigation. While this study addressed this with the Drone Forensic Investigation Model, further studies can further deepen this in line with the rapidly evolving drone landscape.

Furthermore, while commercial tools offer greater range and capabilities than open-source tools, the costs can be prohibitive. There is a need for continued development of capabilities of open-source tools in order to improve the decoding capabilities of flight data. Presentation of artifacts and interactivity of the tools are also areas of potential improvement.

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

Finally, a key challenge encountered in this study was the lack of technical documentations by drone manufacturers. This is a significant challenge given the different proprietary encoding and security/privacy-by-design measures adopted by the manufacturers, most of which are anti-forensic in nature. Specific recommendations can be made to different manufacturers to provide a required minimum set of information on the technical documentation. Alternatively, there can be standardized technical consistency across different manufacturers, for uniformity in key technical aspects to aid incident investigation.

Acknowledgment

This research was conducted at the Laboratory of Digital Footprints Nig. Limited, Abuja, Nigeria. The authors are grateful to management of Digital Footprints Nigeria Ltd for all the technical support.

Funding: "This research received no external funding"

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

References

[1] M. Abulaish and N. A. H. Haldar, "Advances in Digital Forensics Frameworks and Tools," *International Journal of Digital Crime and Forensics*, vol. 10, no. 2, pp. 95–119, Apr. 2018, doi: https://doi.org/10.4018/ijdcf.2018040106.

[2] E. Adorni, A. Rozhok, R. Revetria, and M. Ivanov, "Literature review on drones used in the surveillance field," in *Proceedings of the international multiconference of engineers and computer scientists*, 2021.

[3] N. Ahmad, R. A. R. Ghazilla, N. M. Khairi, and V. Kasi, "Reviews on Various Inertial Measurement Unit (IMU) Sensor Applications," *International Journal of Signal Processing Systems*, vol. 1, no. 2, pp. 256–262, 2013, doi: https://doi.org/10.12720/ijsps.1.2.256-262.

[4] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, "Research Challenges and Opportunities in Drone Forensics Models," *Electronics*, vol. 10, no. 13, p. 1519, Jun. 2021, doi: https://doi.org/10.3390/electronics10131519.

[5] A. Almusayli, T. Zia, and E.-H. Qazi, "Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology," *Technologies*, vol. 12, no. 1, p. 11, Jan. 2024, doi: https://doi.org/10.3390/technologies12010011.

[6] R. Altawy and A. M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, Nov. 2016, doi: https://doi.org/10.1145/3001836.

[7] S. Atkinson, G. Carr, C. Shaw, and S. Zargari, "Drone forensics: The impact and challenges," *Digital Forensic Investigation of Internet of Things (IoT) Devices*, pp. 65–124, 2021.

[8] T. Benarbia and K. Kyamakya, "A Literature Review of Drone-Based Package Delivery Logistics Systems and Their Implementation Feasibility," *Sustainability*, vol. 14, no. 1, p. 360, Dec. 2021.

[9] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington, "Drone forensics: challenges and new insights," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2018, pp. 1–6.

[10] B. Carrier and E. Spafford, "An eventbased digital forensic investigation framework," *Digital Investigation*, 2004.

[11] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," *Digital Investigation*, vol. 22, pp. S3–S14, Aug. 2017, doi: https://doi.org/10.1016/j.diin.2017.06.013.

[12] Data Protection Commission, "Guidance on the Use of Drones," *dataprotection.ie*, May 2022. https://www.dataprotection.ie/sites/default/files/uploads/2022-05/Guidance%20on%20the%20use%20of%20drones%20-%20May%202022%20Final.pdf (accessed Dec. 29, 2023).

[13] Drone Survey Services, "US Drone Statistics 2024," *Drone Survey Services*, 2023. https://dronesurveyservices.com/drone-statistics/

[14] B. Carrier, "Defining digital forensic examination and analysis tools," *Digital Investigation*, 2002.

[15] DJI, "Phantom 3 Professional User Manual v1.8," Jul. 2017. https://dl.djicdn.com/downloads/phantom_3/User%20Manual/Phantom_3_Professional_User_Manual_v1.8_en.pdf (accessed Dec. 28, 2023).

[16] EASA, "EU Wide Rules on Drones published - Safe, secure and sustainable operation of drones," *EASA*, Jun. 11, 2019. https://www.easa.europa.eu/en/newsroom-and-events/press-releases/eu-wide-rules-

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024

drones-published
[17] EASA, "Regulations on UAS (drone) explained," *EASA*, 2019. https://www.easa.europa.eu/en/the-agency/faqs/regulations-uas-drone-explained
[18] EASA, "Civil drones (unmanned aircraft)," *EASA*, 2019. https://www.easa.europa.eu/en/domains/civil-drones
[19] Federal Aviation Administration, "Drones by the Numbers (as of 5/31/23)," *Federal Aviation Administration*, 2023. https://www.faa.gov/node/54496
[20] A. O. Flaglien, "The Digital Forensics Process," *Digital Forensics*, pp. 13–49, May 2017, doi: https://doi.org/10.1002/9781119262442.ch2.
[21] T. Hermawan, Y. Suryanto, F. Alief, and L. Roselina, "Android Forensic Tools Analysis for Unsend Chat on Social Media," *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Dec. 2020, doi: https://doi.org/10.1109/isriti51436.2020.9315364.
[22] Interpol, "Framework for Responding to a Drone Incident for First Responders and Digital Forensics Practitioners," 2020. Available: https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf
[23] F. Iqbal *et al.*, "Drone forensics: examination and analysis," *International Journal of Electronic Security and Digital Forensics*, vol. 11, no. 3, p. 245, 2019, doi: https://doi.org/10.1504/ijesdf.2019.10020543.
[24] P. Jain and A. Mishra, "Extraction of Data using Cellebrite UFED 4PC," *International journal of medical toxicology & legal medicine*, vol. 26, no. 3and4, pp. 222–232, Jan. 2023, doi: https://doi.org/10.5958/0974-4614.2023.00074.8.
[25] G. Kessler and G. Carlton, "A Study of Forensic Imaging in the Absence of Write-Blockers," *Journal of Digital Forensics, Security and Law*, vol. 9, no. 3, 2014, doi: https://doi.org/10.15394/jdfsl.2014.1187.
[26] S. Komasová, "Possible Inspiration: Drone-Related Literature and Its Potential for Public Perception Research," *Journal of Intelligent & Robotic Systems*, vol. 103, no. 3, Oct. 2021, doi: https://doi.org/10.1007/s10846-021-01498-9.
[27] R. Lyda and J. Hamrock, "Using Entropy Analysis to Find Encrypted and Packed Malware," *IEEE Security and Privacy Magazine*, vol. 5, no. 2, pp. 40–45, Mar. 2007, doi: https://doi.org/10.1109/msp.2007.48.
[28] Nigeria Civil Aviation Authority, "Unmanned Aircraft System Operations in Nigeria's Airspace – Guidance. NCAA," *ncaa.gov.ng*, 2019. https://ncaa.gov.ng/documents/advisory-circulars/unmanned-aircraft-system-operations-in-nigeria-s-airspace-guidance/
[29] M. Pollitt, "Computer forensics: An approach to evidence in cyberspace," in *Proceedings of the National Information Systems Security Conference*, 1995, pp. 487–491.
[30] F. E. Salamh, M. M. Mirza, and U. Karabiyik, "UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies," *Electronics*, vol. 10, no. 6, p. 733, Mar. 2021, doi: https://doi.org/10.3390/electronics10060733.
[31] Statista, "Drone Market Revenue worldwide.," *Statista*, 2023. https://www.statista.com/forecasts/1399063/drone-market-revenue-worldwide
[32] S. Tahiri, "Digital Forensics Models," *InfoSec Institute*, Jan. 25, 2016. https://resources.infosecinstitute.com/topic/digital-forensics-models/
[33] S. Viswanathan and Z. Baig, "Digital forensics for drones: A study of tools and techniques," *Applications and Techniques in Information Security: 11th International Conference, ATIS 2020, Brisbane, QLD, Australia, November 12–13, 2020, Proceedings 11*, pp. 29–41, 2020.
[34] O. J. Woodman, "An introduction to inertial navigation," University of Cambridge, Computer Laboratory, 2007.
[35] National Institute of Standards and Technology (NIST), "Computer Forensics Tools & Techniques Catalog," *NIST*, 2023. https://toolcatalog.nist.gov/

DOI: https://doi.org/10.54216/JCIM.150115
Received: February 07, 2024 Revised: April 27, 2024 Accepted: July 29, 2024