Investigating Drone Data Recovery Beyond the Obvious Using Digital Forensics

Smit Chandrakant Nayak, Bharath K. Samanthula and Vaibhavi Tiwari
School of Computing, Montclair State University
1 Normal Ave, Montclair, New Jersey 07043, USA
Email: {nayaks2, samanthulab, tiwariv1}@montclair.edu

***Abstract*—The rapid advancement of drone technology has opened up new opportunities across a wide range of sectors, including agriculture, surveillance, and delivery services. Specifically, the accessibility and affordability of drones suggest a surge in their prevalence in the coming years. Nonetheless, this growth opened new doors for bad actors to use drones for nefarious activities; thereby, raising safety and security concerns attributed to the unmanned aerial vehicles (UAVs). In this paper, we focus on systematically investigating the data recovery mechanisms for confiscated drones. First, we discuss the potential security threats associated with the drones and different detection methods to spot drones. Then, we propose a structured data recovery framework to effectively retrieve crucial data from a malicious drone. In particular, we analyze the popular DJI Mini 2 SE drone and show how our proposed framework can facilitate forensic investigators to uncover crucial data beyond the drone's metadata. Our experiments show that investigators can effectively recover sensitive historical data that was even deleted from the drone's external secure digital (SD) card.**

***Index Terms*—Drone, Attacks, Data Security, Digital Forensics, Data Recovery, SD cards**

I. Introduction

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have emerged as versatile aircrafts with remote and autonomous control capabilites encompassing small sensor devices to large-scale military systems [1], [2]. With a diverse range of sizes and configurations, drones have been used in applications across a wide range of domains including aerial photography, goods delivery, search and rescue missions, and military operations. Figure 1 highlights the statistical data illustrating the drone industry and its various applications [3]. Since drones collect and store valuable data, they bring forth new opportunities and challenges, especially in the areas of safety, security and privacy [4].

On one hand, drones have been commonly used in military operations to penetrate into enemy's airspace and deployed at altitudes of approximately 200 feet above the ground level, although this may vary based on the specific drone and its intended use. Some military drones, for instance, can operate at altitudes of 30,000 feet or higher. Moreover, the duration of flight varies across different drone models. For instance, small tactical drones may only have a flight time of a couple of hours, while larger, more advanced drones can stay aloft for over 24 hours, thus, providing prolonged surveillance and effective combat operations [5]. The confidentiality of the data collected during these military operations, such as flight travel path and reconnaissance footage, needs to be guaranteed at all times. On the other hand, recent advancements in drone technology have not only increased their affordability but also expanded the adoptability of drones in commercial applications. Figure 2 displays the substantial compound annual growth rate (CAGR) of the commercial drone market in recent years [6].

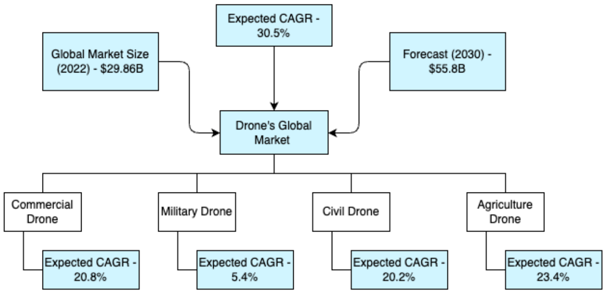


Fig. 1. Statistics for the drone industry

It is worth noting that concerns arise due to the potential misuse of drones for offensive purposes or when drones fell into wrong hands. The delivery of weapons or explosives, reconnaissance activities and surveillance capabilities associated with drones have raised apprehensions among countries and organizations. There exist numerous instances in which drones have been utilized for nefarious activities, including the infringement of no-fly zones, unlawful engagements by criminals, and the deployment of aerial missiles [7]. For example, the drone disruption at Gatwick airport in 2018 and the drone swarm attack on a Russian airbase reflect the potential threats posed by malicious drones. The Gatwick airport incident highlighted the vulnerability of critical infrastructure to drone disruptions, causing significant economic and logistical damage with flight cancellations and diversions affecting thousands of passengers [8]. Similarly, the coordinated drone swarm attack on the Russian airbase demonstrated their potential usage in orchestrated attacks, posing a threat to military installations [9].

979-8-3503-0413-8/23/$31.00 ©2023 IEEE

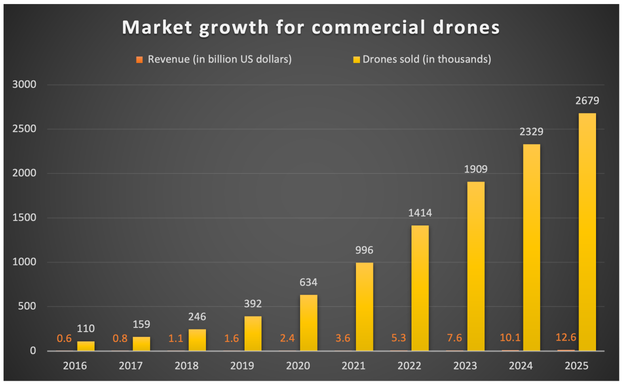


Fig. 2. Market growth for commercial drones

To detect and mitigate potential threats posed by malicious drones, counter-drone technologies and regulatory efforts have intensified in recent years. It is imperative for investigators to conduct forensic analyses on confiscated drones that have been employed for malicious activities [10]. In this paper, we undertake a comprehensive investigation of drone detection strategies and provide a systematic data recovery framework to retrieve different types of data using sound forensic tools. Specifically, we employ well-known digital forensics tools, namely Autopsy, FTK Imager, and DJI Assistance, to show that both deleted and recorded flight data from captured drones can be recovered. Our experimental results clearly show that our framework is very effective and can be a helpful tool in investigator's arsenal for drone forensics.

II. Related Work

The discipline of drone forensics was comprehensively investigated by Yousef et al. [11] emphasizing the need for specialized tools and analysis as drones possess numerous enhancements that pose challenges in the context of digital forensic analysis. Their study revealed that the file systems across various models of DJI drones adhere to consistent standards for media files, EXIF data, spatial movement, metadata, and location [11].

Lan et al. [12] conducted a forensic examination on a DJI Mavic Air 2 unmanned aerial vehicle investigating various scenarios, including an incident involving an abrupt descent. Data was collected from multiple devices implicated in the case, including smartphones, laptops, and the drone's internal memory. They utilized chip-off and chip-on methodologies to acquire data which led to the identification of a board serial number that is classified as Personal Identifiable Information (PII) and associated with the owner/operator of the drone.

A recent study was conducted on commonly used drone models in criminal activities to examine the potential information that could be obtained to enhance law enforcement investigations [13]. Investigators collected various types of data from the six brands, including media files such as images and videos, flight patterns, geographical coordinates, and owner identifications.

Yousef and Iqbal [14] conducted an experiment by utilizing the DJI Mavic Air drone and the iPhone 6 mobile device as the primary tools. Because of temporal limitations, their method was unable to locate the DJI's .DAT and .txt files, which would have furnished pertinent flight data. Hamidi et al. [15] examined the DJI Phantom 4 Standard drone in order to establish a new methodology for analyzing the .DAT file and extracting data from storage sources that could be utilized as evidence in criminal investigations. However, their method has limitations since it is not always accurate. They also recommended to further explore alternative drone models and emphasized the need for additional investigation to understand the intricacies of .DAT and .txt file formats [15].

A recent case study [16] emphasized significant disparities in the functionalities of commonly utilized UAV forensic software and tools. They observed that the DatCon tool can successfully decrypt the .DAT file and transform it into a readable CSV file. However, it is worth noting that the efficacy of other tools employed in their study for decrypting .DAT files, even when utilized with the DatCon module, exhibited inconsistent outcomes. Their work emphasizes the significance of validating and corroborating findings through the utilization of multiple tools.

Existing drone forensic work has largely focused on extracting information from the data collected and stored directly by an unmanned aerial vehicle (UAV). In our proposed framework, we extend our forensic analysis beyond the mere extraction of the drone's metadata by analyzing and recovering historical data associated with the SD card. It is worth noting that retrieving historical data in criminal investigations can offer significant benefits, for example, information about past users who have accessed the SD card can uncover new details useful in identifying culprits.

III. Drone Detection Methods

In this section, we provide an overview of the widely adopted methods to detect the presence of a drone at a given location and analyze the activities being carried out. Some important components of drones and their corresponding features are given in Table I.

(a). *Drone Detection Systems* - These systems utilize a variety of technologies, such as radar, radio frequency (RF) sensors, and optical sensors, to detect the presence of drones in the airspace. They can identify and track drones based on their RF signatures, flight patterns, or visual characteristics [17].

(b). *RF Signal Analysis* - By monitoring the RF spectrum, it is possible to detect and analyze the communication signals used by drones. This technique involves capturing and analyzing the radio signals emitted by drones, including their control signals and video transmission, to identify unauthorized or malicious activities [18].

TABLE I
COMMON DRONE COMPONENTS AND CHARACTERISTICS

Drone Parts	**Drone Features**
Flight controller	Cameras, Flight records
GPS module	Artificial intelligence modeling
Antenna	Maximum flight time
Battery	Media storage format
Receiver	Maximum climb and descent rates
Speed limiters	Augmented reality features
Ultrasonic sensor	Hover accuracy
Collision avoidance sensors	Sensory range of obstructions
Altimeter sensor	Live video feed
Accelerometer sensor	Ability to maintain a constant altitude

(c). *Video Analytics* - Video analytic techniques use computer vision algorithms to analyze live or recorded video footage captured by surveillance cameras [19]. These algorithms can detect and track drones based on their visual features, such as their shape, size, and movement patterns, enabling the identification of potential threats or suspicious activities.

(d). *Thermal Image Analysis* - This involves the utilization of a thermal camera to recognize the significant amount of radiated heat emitted by the internal components of a drone. This approach has paved the way for several methodologies aimed at detecting drones based on their unique heat signatures [20]. Specifically, the application of convolution neural networks (CNNs) has been employed to enhance the performance and improve the detection accuracy of UAVs from thermal images [21]. The thermal image-based drone detection approach offers various advantages, including availability for identification, resilience to different weather conditions, and cost-effectiveness compared to radar detection systems. However, it is worth noting that the detection range of thermal-based systems is typically limited to a maximum of 51 meters, which is shorter compared to most other detection approaches.

(e). *Acoustic Analysis* - This technique involves estimating the unique acoustic signatures generated by the internal components of a drone, such as motors and fast-rotating propellers. By utilizing different acoustic systems, researchers have developed a variety of methodologies for detecting, classifying, and localizing drones [22].

(f). *Geofencing and Airspace Monitoring* - Geofencing is a technique that uses GPS or other positioning systems to create virtual boundaries around sensitive areas or restricted airspace. By deploying geofencing technologies, it is possible to detect and prevent drones from entering prohibited zones, providing an additional layer of security [23].

IV. DATA RECOVERY METHODS FOR DRONES

(a). *Physical Data Recovery* - Engaging with the drone's tangible storage mechanisms, physical data recovery necessitates direct interfacing with its components. This may encompass the utilization of dedicated hardware and software mechanisms to probe storage modalities such as Secure Digital (SD) cards and hard disk drives [24]. Plus, component replacement deals with substituting malfunctioned storage units to facilitate data extraction. Furthermore, the chip-off method mandates the detachment of memory microchips, permitting the direct acquisition of data through advanced apparatuses.

(b). *Software Driven Data Recovery* - Pivoting on software frameworks, these methodologies are anchored in extracting data via the drone's software constructs and file systems [25]. File system recovery is predicated on the dissection of the drone's file system, aiming to identify and restore uncorrupted files and directories. The purview of deleted data recovery spans the reclamation of data previously erased or formatted, capitalizing on the residual footprints. Data carving is orchestrated to salvage segmented or unallocated datasets by pinpointing file signatures and subsequent recompilation. Anomaly detection software tools invoke machine learning algorithms to decode aberrant data trajectories and facilitate data restoration [26].

(c). *Forensic Data Recovery* - Forensic modalities plunge into a meticulous examination of the drone's memory infrastructure and associated metadata [27]. Memory scrutiny disentangles data housed within volatile memory units (RAM), spotlighting active or transiently processed datasets. Timeline reconstruction meticulously curates a sequential chronology demystifying antecedents to data compromise. Furthermore, metadata investigation pivots on the extraction and subsequent analytical scrutiny of metadata intrinsic to the drone-mediated data, and thus, facilitating event reconstruction.

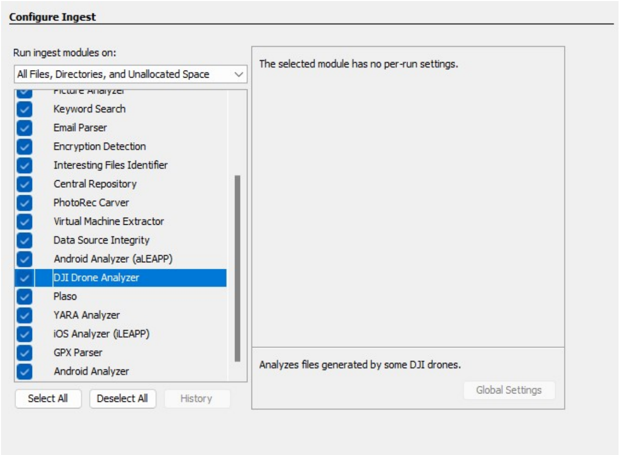
(d). *Cloud Focused Data Recovery* - Central to this modality is the probative analysis of cloud repositories affiliated with the drone. Such an investigation can reveal data either synchronized or archived in the backup storage on cloud. Moreover, the analysis of remote data purge commands transmitted to the drone could be emblematic of scenarios precipitating to data compromise, unauthorized activity or privacy violation [28].

V. THE PROPOSED METHODOLOGY

In this section, we present a novel approach that focuses on two distinct methods for extracting information from drones. The first method utilizes metadata sourced directly from the drone, while the second method extracts information from the drone's secondary storage device (e.g., an SD card). At the core of our proposed solution, we utilize the Autopsy digital forensic tool.

A. An Overview of Autopsy

The Autopsy platform, created and managed by Basis Technology Corp, is a freely available open-source digital



Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity
- ☑ Android Analyzer (aLEAPP)
- ☑ DJI Drone Analyzer
- ☑ Plaso
- ☑ YARA Analyzer
- ☑ iOS Analyzer (iLEAPP)
- ☑ GPX Parser
- ☑ Android Analyzer

The selected module has no per-run settings.

Analyzes files generated by some DJI drones.

Fig. 3. Drone analyzer feature within the Autopsy digital forensic tool

forensics tool. It functions as a graphical user interface for The Sleuth Kit and various other digital forensic modules [29]. The platform has been prevelant among military, law enforcement, and private industry auditors for the purpose of examining computer and network activities. The Autopsy tool encompasses a variety of indispensable features which are crucial for an efficient and accurate forensic analysis through its interactive graphical interface. Some popular features of Autopsy are highlighted below.

- *Timeline Analysis* - An interface that enables advanced graphical event viewing.
- *Drone Analyzer module* - A feature that allows the analysis of files from drones. Figure 3 depicts the visual representation of the drone analyzer feature as it appears within the Autopsy tool.
- *Data Carving* - The capability to recover deleted files from un-allocated space is a valuable feature that proves beneficial in extracting data, especially when data lost due to a ransomware attack [30].
- *Hash Filtering* - This feature helps with the identification of known malicious files through hash signatures, while disregarding known good files.
- *Keyword Search* - Indexed keyword search functionality for locating documents that contain relevant terms.
- *Web Artifacts* - A feature that allows extraction of browser history, bookmarks, and cookies.

B. The Proposed DDRH Framework

In this sub-section, we present a novel and systematic methodology for extracting valuable information from drones by utilizing the Autopsy tool. We refer to our new solution as **D**rone **D**ata **R**ecovery with **H**istorical data (DDRH) framework. Our framework consists of three main phases: (i) Disk Image Creation, (ii) Disk Image Loading and Analysis, and (iii) Data Extraction. Next, we discuss the key steps involved in each phase below.

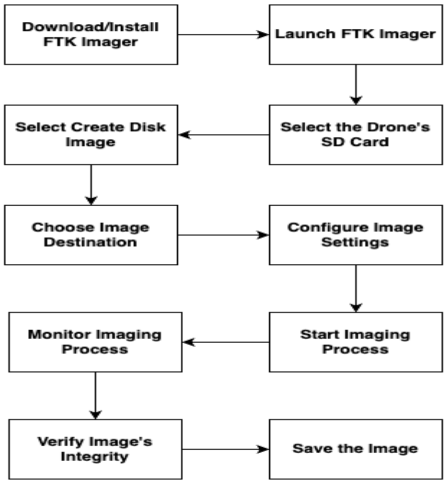


Fig. 4. Proposed flowchart for disk image creation

(a). *Phase 1 - Disk Image Creation*: To facilitate the forensic analysis of the captured drone and the extraction of its data, the first phase is to essentially create a proper disk image of the device. This phase requires a series of steps as outlined in Figure 4.

(b). *Phase 2 - Disk Image Loading and Analysis*: Upon the creation of a disk image, the next phase involves importing the disk image into the Autopsy tool. Once the image is loaded, the Autopsy software commences an automated procedure aimed at analyzing the image data and extracting significant details. This process involves retrieving various relevant pieces of information, such as the duration of the flight, GPS tracking data, geolocation history, and other pertinent data points. Moreover, Autopsy provides a key feature known as data carving, which enables the recovery of deleted media data. This module proves to be advantageous to forensic investigators as it helps them to retrieve supplementary information, such as historical data, based on specific criteria (more details are provided in Section VI). Figure 5 illustrates a compilation of the essential procedures involved during the forensic analysis of a drone.

(c). *Phase 3 - Data Extraction*: After analyzing the image file with Autopsy, a variety of files become visible on the left side of the Autopsy interface. To retrieve the data, one can simply right-click on the file's name and opt for the "extract files" feature. This action restores the file to its original format. An illustrative depiction of this data extraction procedure is shown in Figure 6. Note that the drone analyzer capability within Autopsy serves as a means to achieve efficient file extraction. Moreover, Autopsy's geolocation functionality is applicable for assessing both the geographic positioning of the device and the sequential progression of activities within the system. This dual-purpose feature aids in pinpointing the timing of specific actions and their corresponding geographic contexts.

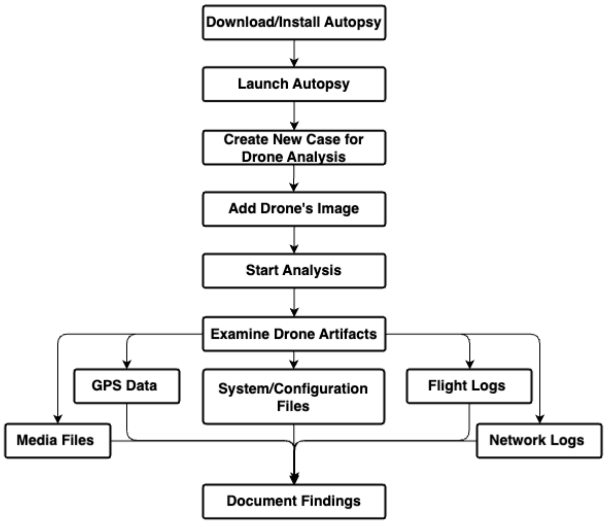
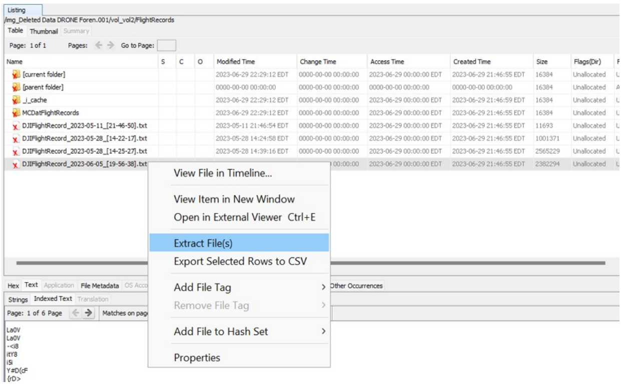


Fig. 5. Step-by-Step process for forensic analysis of a drone using Autopsy



/img_Deleted Data DRONE Foren.001/vol_vol2/FlightRecords

Page: 1 of 1

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
[current folder]				2023-06-29 22:29:12 EDT	0000-00-00 00:00:00	2023-06-29 00:00:00 EDT	2023-06-29 21:46:55 EDT	16384	Unallocated	U
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16384	Unallocated	A
_i_cache				2023-06-29 22:29:12 EDT	0000-00-00 00:00:00	2023-06-29 00:00:00 EDT	2023-06-29 21:46:59 EDT	16384	Unallocated	U
MCDatFlightRecords				2023-06-29 22:29:12 EDT	0000-00-00 00:00:00	2023-06-29 00:00:00 EDT	2023-06-29 21:46:55 EDT	16384	Unallocated	U
DJIFlightRecord_2023-05-11_[21-46-50].txt				2023-05-11 21:46:54 EDT	0000-00-00 00:00:00	2023-06-29 00:00:00 EDT	2023-06-29 21:46:55 EDT	11693	Unallocated	U
DJIFlightRecord_2023-05-28_[14-22-17].txt				2023-05-28 14:24:58 EDT	0000-00-00 00:00:00	2023-06-29 00:00:00 EDT	2023-06-29 21:46:55 EDT	1001371	Unallocated	U
DJIFlightRecord_2023-05-28_[14-25-27].txt				2023-05-28 14:39:16 EDT	0000-00-00 00:00:00	2023-06-29 00:00:00 EDT	2023-06-29 21:46:55 EDT	2565229	Unallocated	U
DJIFlightRecord_2023-06-05_[19-56-38].txt					00:00:00	2023-06-29 00:00:00 EDT	2023-06-29 21:46:55 EDT	2382294	Unallocated	U

Page: 1 of 6 Page

```
La0V
La0V
-<i8
itY8
i5i
Y#D(cF
{rD>
```

Fig. 6. Extraction of a deleted file using the Autopsy tool

VI. Experimental Results

In this section, we present two types of experimental results based on the proposed DDRH framework. The first experiment focuses on retrieving different metadata from the drone, a feat achieved even in instances where the said data has been deliberately deleted. The second experiment focuses on extracting critical historical information associated with the SD card utilized by the drone under consideration.

A. System Setup

In our experiments, we utilize a DJI drone to perform extensive forensic analysis. The selection of the DJI drone was motivated by its widespread adoption across a multitude of industries; thus, demonstrating the practical applicability of our results. Table II summarizes the principal attributes [31] of the drone utilized in our experiments.

In addition to the DJI Mini 2 SE drone, we employed an Apple iOS mobile device as a means of controlling and maneuvering it from a remote location. Specifically, the device was used to control movement of the drone, capture visual media, access intelligent flight modes, and configure various settings. Table III highlights the features associated with the mobile device used.

TABLE II
Characteristics of the DJI Drone

Attribute	Description
Model	DJI Mini 2 SE
Weight	249 g
Max Ascent Speed	5 m/s
Max Descent Speed	3.5 m/s
Max Flight Time	31 minutes
Navigation System	GPS + GLONASS + Galileo
Image Sensor	1/2.3-inch CMOS, Effective Pixels: 12 MP
Photo Format	JPEG/DNG (RAW)
Video Format	MP4 (MPEG-4 AVC/H.264)
Video Transmission System	DJI O2
Battery Capacity	2250 mAh
External Storage	32 GB Samsung Memory Card

TABLE III
Characteristics of the Mobile Device used

Feature	Description
Model	iPhone 13 Pro Max
OS Version	iOS 16.5
Storage Capacity	256 GB
Display	6.7-inch Super Retina XDR
Processor	A15 Bionic chip with 6-core CPU
Camera System	Telephoto, Wide, and Ultra Wide
Battery	Built-in rechargeable lithium-ion battery
Network Support	5G support

B. Metadata Analysis

In this sub-section, we present a thorough empirical analysis of the proposed DDRH methodology for extracting metadata. We emphasize that DDRH successfully facilitated us to retrieve both extant and erased data collected by the drone.

1) Recovery of Flight Log Data: The flight logs consist of a wide spectrum of data, encompassing parameters related to flight, sensor measurements, control commands, system states, and supplementary information. These logs collectively form an exhaustive documentation of the drone's operational behaviors during its flight trajectory. They furnish indispensable insights into a variety of parameters, including altitude, speed, orientation, battery health, and any deviations or anomalies noted during the course of the flight. By leveraging the capabilities of the Autopsy tool, we successfully extracted all essential flight log data. Table IV presents a summary of the retrieved flight data.

2) Recovery of GPS Data: In order to obtain the precise and reliable data pertaining to the spatial coordinates of the drone, we employed the geo-location functionality offered by Autopsy. Table V presents a comprehensive summary of the retrieved GPS data.

TABLE IV
RECOVERED FLIGHT LOG DATA

Device Name	DJI Mini 2 SE
Timestamp	June 1st, 2023 8:25 PM
Flight Air Time	11m 59s
Take Off Battery	93 Percent
Landing Battery	49 Percent
Total Mileage	2740 ft
Maximum Altitude Gained	133.5 ft
Maximum Speed Gained	17.40 mph
Tips During Flight	14
Warnings During Flight	8
Maximum Temperature	110.8 F

TABLE V
RECOVERED GPS DATA

Take Off Latitude	40.456493
Take Off Longitude	-74.498831
Zip Code	08902
State, Country	New Jersey, United States
Last Known Latitude	40.456493
Last Known Longitude	-74.498837
Log Duration	12m 01s
Air Duration	11m 59s

The flight path information retrieved by using the geo-location feature is illustrated in Figure 7. The line that is highlighted in green depicts the complete trajectory of the flight. The battery condition of the drone during flight is indicated by the presence of a blue battery icon. The green balloon icons symbolize the designated safe altitude, whereas the orange balloon icon represents the maximum altitude that can be maintained during the course of the flight.

3) Recovery of Media Files: To further evaluate the effectiveness of our framework in retrieving the data from the disk image, we utilized a dataset of 73 media files recorded by our drone. Table VI shows the list of file types and formats from our dataset. Before the disk image was created, we intentionally removed 69 of these files. We then analyzed the disk image with the Autopsy tool to extract the deleted media files. It is worth noting that our DDRH framework effectively recovered all the 69 deleted files.

C. SD Card Analysis

In this sub-section, we provide a comprehensive examination of the proposed methodology for extracting information pertaining to the SD card attached to our drone.

1) Retrieval of SD Card Device History: After analyzing the disk image of the SD card, we successfully recovered data about the devices where the card had previously been used for storage. Specifically, our findings revealed that the SD card had been in use since 2016. Plus, the card was used in five devices prior to its installation in the drone. We managed to extract information about these previous devices and their classifications. Out of the five devices, two were DSLR cameras, and three were Android phones. Additionally, we were able to effectively retrieve the time period during which the SD card was utilized in all the five devices. The results are shown in Table VII.

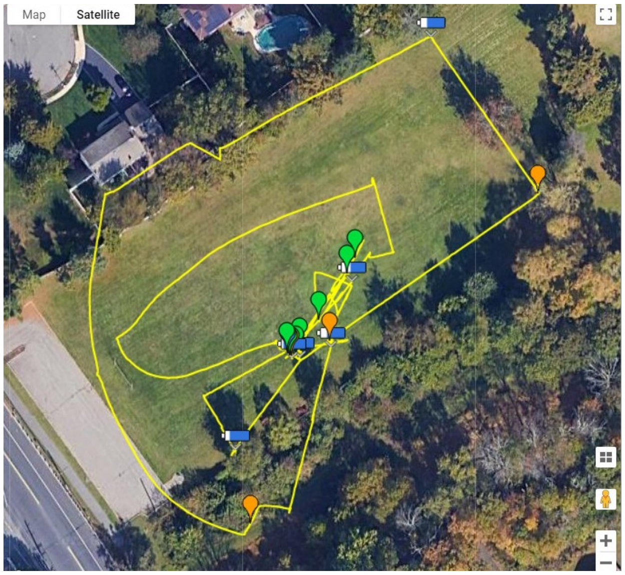


Fig. 7. A snapshot of the drone flight path

2) Recovery of SD Card Historical Data: We conducted further investigation on the SD card to retrieve deleted media files and information associated to the previous owners of the SD card. The SD card being examined contained a total of 25,480 files before it was used in the drone. It is worth mentioning that all the 25,480 files were deleted before utilizing the SD card for the drone. The deleted files encompassed a wide array of types, including image files, video files, audio files, database files, system files, and contact files. The investigation was effectively carried out, leading to the retrieval of all deleted files from the SD card. The list of different file types and their corresponding counts are given in Table VIII.

TABLE VI
LIST OF MEDIA FILE FORMATS

File Types	**Number of Files**	**Formats**
Image Files	61	JPEG
Video Files	4	MP4
Log Files	8	DAT

TABLE VII
LIST OF DEVICES PREVIOUSLY USED THE DRONE'S SD CARD

Device Name	**Model**	**Used From**	**Used Until**
Canon	Canon EOS 1200D	09-12-2017	09-13-2017
Motorola	Moto G 5S Plus	01-13-2016	06-20-2016
Samsung	SM-N910G	06-21-2016	06-25-2018
Nikon	Nikon D5300	06-30-2018	06-30-2018
Samsung	SM-G885F	09-30-2018	05-21-2022

TABLE VIII
LIST OF SD CARD'S OLD MEDIA FILES RECOVERED

Retrieved File Types	Count of Retrieved Files
Image Files	5624
Video Files	372
Orphan Files	16028
System Files	1529
Audio Files	623
Database Files	14
PDF Files	79
Contacts	950
Application Files	261

D. Discussions

Despite the SD card being utilized across various devices and formatted before using it for the drone, our empirical results show that we can effectively trace and retrieve critical historical data. For example, through our systematic forensic analysis, we successfully obtained contact information of 950 individuals. This information plays a significant role in assisting the law enforcement agents to fast-track criminal cases and trace to the potential suspects linked to the malicious drone under investigation. On the contrary, if a drone falls into the wrong hands, we emphasize that leaking such sensitive information to unauthorized users pose a potential risk.

VII. CONCLUSIONS

The rise of drone technology and their extensive use in military operations, agriculture, photography and logistics, make them an indispensable tool in the skies. However, as the drones become more affordable, there has been significant increase of drone usage in criminal or harmful activities. In this paper, we proposed a novel data recovery framework for drones that can facilitate forensic investigators to extract both metadata and historical data associated with the drone's SD card. Our experimental results using the DJI Mini 2 SE drone demonstrated the effectiveness of our sound forensic approach. As drones reshape industries, we claim that our work guides their integration for a safer world.

As a future work, we will extend our method to detect and recover data from drones impacted with denial of service and ransomware attacks. Plus, we will investigate the applicability of our framework under a cloud-based drone setting.

REFERENCES

[1] L. Dormehl. (2018) The history of drones in 10 milestones. [Online]. Available: https://www.digitaltrends.com/cool-tech/history-of-drones/

[2] M. Alwateer, S. W. Loke, and A. M. Zuchowicz, "Drone services: Issues in drones for location-based services from human-drone interaction to information processing," *J. LBS*, vol. 13, pp. 94–127, 2019.

[3] D. I. Insights, "Drone market analysis 2022-2030." [Online]. Available: https://droneii.com/drone-market-analysis-2022-2030

[4] D. Kovar and J. Bollo, "Drone forensics," *Digital Forensics Magazine*, vol. v34, pp. 14–19, 2018.

[5] "Unmanned aircraft system (uas) categories," Air Domain Intelligence. [Online]. Available: https://www.airdomainintelligence.mil/Global-Air-Hub/Unmanned-Aircraft-System-UAS/UAS-Categories/

[6] M. Carlier, "Commercial drone market revenue worldwide projection," Statista, May 2 2023. [Online]. Available: https://www.statista.com/statistics/607922/commercial-drone-market-revenue-worldwide-projection/

[7] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington, "Drone forensics: Challenges and new insights," in *Proceedings of the NTMS*. Paris, France: IEEE, February 2018, pp. 1–6.

[8] A. Haylen, "Civilian drones," Briefing Paper No. CBP 7734, 2019, retrieved from www.parliament.uk/commons-library.

[9] "Syria war: Russia thwarts drone attack on hmeimim airbase," 2018. [Online]. Available: https://www.bbc.com/news/world-europe-42595184

[10] U. Jain, "A drone forensics investigation framework," Ph.D. dissertation, Purdue University, West Lafayette, IN, USA, 2017.

[11] M. Yousef, F. Iqbal, and M. Hussain, "Drone forensics: A detailed analysis of emerging dji models," in *Proceedings of the 11th International Conference on Information and Communication Systems (ICICS)*, Irbid, Jordan, April 2020, pp. 066–071.

[12] J. K. W. Lan and F. K. W. Lee, "Drone forensics: A case study on dji mavic air 2," in *Proceedings of the International Conference on Advanced Communication Technology*, February 2021, pp. 291–296.

[13] K. Al-Room, F. Iqbal, T. Baker, B. Shah, B. Yankson, A. MacDermott, and P. C. Hung, "Drone forensics: A case study of digital forensic investigations conducted on common drone models," *International Journal of Digital Crime and Forensics*, vol. 13, pp. 1–25, 2021.

[14] M. Yousef and F. Iqbal, "Drone forensics: A case study on a DJI Mavic Air," in *Proceedings of the AICCSA*, 2019, pp. 1–3.

[15] F. Iqbal, S. Alam, A. Kazim, i. MacDermott, and D. A. Hamdi, "Drone forensics: A case study on DJI Phantom 4," in *Proceedings of the AICCSA*, 2019, pp. 1–6.

[16] 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, 2021.

[17] P. Molchanov, R. I. Harmanny, J. J. de Wit, K. Egiazarian, and J. Astola, "Classification of small uavs and birds by micro-doppler signatures," *Int. J. Microw. Wirel. Technol*, vol. 6, pp. 435–444, 2014.

[18] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu, "Cost-effective and passive rf-based drone presence detection and characterization," *Mobile Comp. Comm*, vol. 21, pp. 30–34, 2018.

[19] D. S. R. Ganti and Y. Kim, "Implementation of detection and tracking mechanism for small uas," in *ICUAS*, 2016, pp. 1254–1260.

[20] P. Andrasi, T. Radisic, M. Mustra, and J. Ivosevic, "Night-time detection of uavs using thermal infrared camera," *Transp. Res. Procedia*, vol. 28, pp. 183–190, January 2017.

[21] Y. Wang, Y.-Y. Chen, J. Choi, and C.-C. J. Kuo, "Towards visible and thermal drone monitoring with convolutional neural networks," *APSIPA Trans. Signal Inf. Process*, vol. 8, pp. 1–13, January 2019.

[22] J. Mezei and A. Molnár, "Drone sound detection by correlation," in *Proceedings of the IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2016, pp. 509–518.

[23] S. Zhang, D. Wei, M. Q. Huynh, T. Q. S. Quek, X. Ma, and L. Xie, "Model predictive control based dynamic geofence system for unmanned aerial vehicles," in *AIAA Inf. Syst.-AIAA Infotech Aerosp.*, 2017.

[24] D. Kovar, G. Dominguez, and C. Murphy, "Uav (aka drone) forensics," in *the SANS DFIR Summit*, Austin, TX, USA, 2016, pp. 23–24.

[25] M. Llewellyn, "Dji phantom 3-drone forensic data exploration," *Edith Cowan University; Perth, Australia*, 2017.

[26] I. Nemer, T. Sheltami, I. Ahmad, A. U.-H. Yasar, and M. A.-R. Abdeen, "Rf-based uav detection and identification using hierarchical learning approach," *Sensors*, vol. 21, p. 1947, 2021.

[27] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (uav/drone) forensic framework," *Digital Investigation*, vol. 30, p. 52–72, 2019.

[28] C. Guttman, "Drones connect to cloud computing to analyze data from the sky," *The Forecast by Nutanix*, June 2022. [Online]. Available: https://www.nutanix.com/theforecastbynutanix/technology/drones-connect-to-cloud-computing-to-analyze-data-from-the-sky

[29] The Sleuth Kit. (2020, April 8) Autopsy drone forensics - user documentation. [Online]. Available: https://sleuthkit.org/autopsy/docs/user-docs/4.14.0/drone_page.html

[30] S. C. Nayak, V. Tiwari, and B. K. Samanthula, "Review of ransomware attacks and a data recovery framework using autopsy digital forensics platform," in *IEEE CCWC*, 2023, pp. 605–611.

[31] DJI. (2023) DJI Mini 2 SE. [Online]. Available: https://www.dji.com/mini-2-se