Forensics Case studies – Extraction of deleted and live data from DJI Drone Matrix 600 Pro Through Chip-off, Internal SD Card and Mobile Phone Extraction.

ANKIT[1], HARSH KUMAR SINGHAL[2]
[1, 2]*Digital Forensics Analyst*

Abstract*— The increasing popularity of drones, also known as Unmanned Aerial Vehicles (UAVs), has raised concerns about their potential misuse in criminal activities. This research investigates the forensic analysis of drones, focusing on the extraction and correlation of data from multiple sources, including the drone's internal storage, SD card, mobile phone, and controller, with the aim of establishing connections between the drone and criminal activity. By applying advanced forensic tools such as FTK Imager, Autopsy, Magnet AXIOM Cyber, and Wireshark, we explore methods for retrieving GPS data, user interactions, flight logs, and media files, as well as information from connected devices. Our methodology includes extracting and imaging data from the drone's internal microSD card and mobile devices, processing flight data to reconstruct flight paths, and analyzing system logs to identify key forensic evidence. Additionally, we explore the role of battery voltage data in estimating drone speed and correlating performance metrics during various flight stages. The results demonstrate how digital traces left by drones and their controllers can provide invaluable insights into criminal investigations. This research underscores the growing importance of drone forensics in law enforcement, offering a comprehensive framework for analyzing digital evidence and supporting the identification and prosecution of perpetrators involved in illicit drone-related activities.

I. INTRODUCTION

In recent years, the use of drones has expanded rapidly across various industries, including surveillance, agriculture, photography, and even criminal activity. As drones become increasingly accessible and sophisticated, they have also emerged as a valuable tool in criminal investigations, providing both critical evidence and insights into illicit activities. Drones, equipped with high-resolution cameras, sensors, and advanced flight control systems, generate vast amounts of digital data, which can be used to reconstruct events, identify perpetrators, and provide forensic evidence that was previously unavailable.

The forensic analysis of drones has thus become an essential discipline within digital forensics, particularly in criminal investigations where drones are suspected to be involved. This research paper explores the forensic methodology used to analyze data retrieved from drones, focusing on the tools and techniques employed to extract valuable information from the drone's internal storage, mobile applications, and connected devices. The study incorporates the principles of digital forensics, including the application of Wi-Fi packet analysis and the Locard Exchange Principle, to establish a framework for understanding how drones, their controllers, and their operators leave behind critical digital traces.

The research delves into the process of acquiring and analyzing data from drones, mobile devices, and associated internal microSD cards, using tools such as FTK Imager, Autopsy, and Magnet AXIOM Cyber. These tools enable investigators to extract essential data such as GPS coordinates, flight logs, communication records, user details, and media files, all of which play a crucial role in solving crimes related to surveillance, smuggling, terrorism, and other unlawful activities.

Through a comprehensive exploration of drone forensics, this paper aims to highlight the growing importance of drones as both tools and evidence in criminal investigations, demonstrating how digital evidence from drones can significantly support law enforcement agencies in their efforts to solve crimes. By utilizing advanced forensic techniques, investigators can uncover hidden patterns, reconstruct flight paths, and establish timelines that are pivotal in

connecting suspects to criminal actions. This research ultimately seeks to underscore the evolving role of drone forensics in the modern landscape of digital criminal investigations.

II. PROCEDURE FOR PAPER SUBMISSION

A. Review Stage

1.1. Drone

The basic equipment inside the drone includes the following items: SD card, internal storage, flight control system, sensors, controller, CGO3+ Gimbal Camera, battery, and motor. Some of these items may be critical in drone investigations.

1. SD card and Internal Storage

Photos and videos taken by the drone in flight mode are stored in SD card. The flight log TXT files or DAT files that record GPS (Global Positioning System) coordinates, timestamp, motor speed, and other data are stored in the internal storage of the drone.

2. Flight Control System

Through a flight control system, Wi-Fi information of a drone can be set or modified. The flight data files stored in the drone internal SD card storage can be downloaded. The function of flight settings is provided by a flight control system.

3. Sensors

The drone relies on sensors such as controllers, gyroscopes, accelerometers, and barometers to stabilize the body. With GPS and barometer data, the drone can be locked in the specified position and height.

4. Controller

A controller is used to control the direction and speed of the flight by radio signals. It is usually cooperated with the mobile phone or replaced with a mobile phone.

1.2 Drone Crime Questions

A well-written report of crime investigation tells a story that answers the 5W1H (who, what, when, where, why, and how) questions to identify key issues related to a crime or incident. At the beginning of drone investigation, a careful analysis must be made of some questions that are being asked. The 5W1H formula sets the following objectives.

(1) Who: Persons involved in the investigation, including suspects, witnesses, and victims. Based on collected flight data, this study aims to identify the user of a drone.

(2) Where: The location of the crime and other relevant locations. This study previsualizes the flight path with GPS data.

(3) What: Description of the facts of the crime in question

(4) When: The time of the crime and other related events. This study lists the timestamp of every flight and compares the temporal record between a drone and mobile phone.

(5) Why: The motivation for the crime and why it happened at a given time

(6) How: How the crime was committed?

CASE STUDY

The Increasing Need for Forensic Analysis of Drones in Criminal Investigations

The need for forensic analysis of drones has grown significantly, particularly in the context of criminal investigations. Drones, equipped with cameras, sensors, and sophisticated communication systems, can provide invaluable digital evidence that may aid in identifying suspects or reconstructing criminal events. The data retrieved from drone controllers, mobile phones, or the drones themselves can offer critical insights into a suspect's actions, flight path, and intentions. This evidence, when properly analysed, can play a crucial role in solving crimes involving surveillance, smuggling, terrorism, or other illicit activities.

The foundational principle guiding forensic investigations, the Locard Exchange Principle, posits that "with contact between two items, there is always a transfer of material." This principle, originating in physical forensics, holds significant relevance in the digital forensics field, especially when investigating drones. In the case of drones, the controller or mobile phone used to operate the drone serves as the primary

tool for initiating and maintaining the drone's flight path. The Wi-Fi or radio signals that connect the drone with the controller or mobile device form the digital connection that enables the transfer of data between them. This interaction leaves behind digital evidence, including flight logs, GPS coordinates, video recordings, and other metadata that can be crucial for investigators.

Thus, the analysis of data exchanged between drones and their controllers or mobile devices is essential for modern digital forensics. This research paper will explore the methods used to capture, preserve, and analyse drone-related data, with a focus on the application of Wi-Fi packet analysis through tools like Wireshark. It will also examine the implications of the Locard Exchange Principle in digital contexts, providing a framework for understanding how drones and their operators leave digital traces that can be used to link suspects to criminal activity.

By leveraging digital forensics techniques, investigators can obtain a more detailed understanding of drone-related incidents, leading to the identification of perpetrators and the successful resolution of cases. Ultimately, this paper seeks to highlight the growing importance of drone forensics in law enforcement and explore how digital evidence from drones can be systematically used to support criminal investigations.

Hardware

- Drone
- Mobile Phone
- SD Card

Software

- FTK Imager
- Autopsy
- Magnet Axiom Cyber
- DatCon

Data we get

A. Drone battery voltage of drone that can help me height of drone

In drone forensics or performance analysis, examining battery voltage drops can be useful for checking the drone's speed and overall power usage. Here's how voltage drop data can contribute to speed checking and performance evaluation:

1. Power Consumption Correlation with Speed

- Higher Power Draw at Higher Speeds: Generally, drones consume more power (and thus experience more significant voltage drops) when flying at higher speeds. By examining the battery voltage over time, you can correlate sudden voltage drops with periods of increased speed, such as during rapid acceleration or when the drone is maintaining high-speed flight.
- Energy Usage: A large voltage drop could indicate that the drone is drawing more power, possibly due to high-speed flight, high wind resistance, or a heavy payload. Comparing voltage data at various points during the flight can help estimate the drone's speed at those moments.

2. Estimating Speed Based on Power Usage

- Voltage Drop Rate and Power Demand: When the drone operates at higher speeds, the motor demands more power, resulting in a steeper voltage drop. By examining the rate at which the voltage drops and comparing it to typical flight profiles, forensics or performance experts can estimate the speed at which the drone was traveling. For example, significant voltage drops might coincide with moments when the drone is moving faster, especially in more demanding flight conditions (e.g., rapid climbs or high winds).

3. Battery Voltage Behavior Under Load

- Flight Load and Speed Impact: At lower speeds or during hover, the drone's battery voltage may remain more stable, as power demand is lower. However, during high-speed maneuvers, voltage typically drops more noticeably. By analyzing this voltage behavior, experts can infer if the drone was likely traveling at high speeds at specific moments based on the intensity of voltage drops.

4. Voltage Drop Recovery and Speed Analysis

- Acceleration and Deceleration Patterns: Sudden drops in voltage could coincide with rapid acceleration, where the motors demand more power to increase speed. After the drone reaches a steady cruising speed or decelerates, the voltage may stabilize or recover. By identifying these patterns, forensics experts can correlate voltage fluctuations with specific phases of speed changes during the flight.

5. Comparing Different Speed Segments

- High-Speed vs Low-Speed Segments: During different parts of a flight, the voltage will drop more or less depending on the speed. By separating the data into low-speed and high-speed segments, forensic experts can assess whether the voltage drop aligns with the expected power consumption for each segment. This can help determine the consistency of the drone's speed or identify anomalies that might suggest mechanical issues (e.g., a malfunctioning motor causing higher-than-expected power consumption).

6. Drone Telemetry and Voltage Logs

- Integrated Flight Data: Many drones record telemetry data that includes both speed and battery voltage levels. By analyzing this data together, you can cross-reference the speed readings (GPS data or internal speed metrics) with voltage drops. If the drone's speed spikes and the voltage drops significantly during that time, it reinforces the connection between power demand and speed.

7. Environmental Factors and Their Effect on Speed

- Wind and External Forces: External factors, such as wind resistance or heavy payloads, can impact both speed and battery performance. A strong headwind, for example, would require the drone to consume more power to maintain speed, resulting in a sharper voltage drop. By analyzing these drops in relation to the drone's GPS speed data, investigators can infer the effect of environmental factors on the drone's speed performance.

8. Speed Monitoring Software

- Voltage Monitoring Systems: Many modern drones include telemetry systems that log not only battery voltage but also other performance metrics like motor speed, GPS speed, and altitude. By analyzing these readings in combination, it becomes easier to correlate specific battery voltage drops with moments of high-speed flight.

9. Detecting Speed Anomalies

- Identifying Unusual Flight Behavior: If there are unexpected or unexplained voltage drops, they could indicate anomalies in flight speed. For example, if a drone is operating at a lower speed than expected but still shows significant voltage drops, this could suggest inefficient motor performance or other mechanical issues impacting speed and power consumption.

10. Battery Efficiency at Different Speeds

- Battery Load vs Speed Efficiency: Drones have different power efficiency at varying speeds. Typically, drones consume more battery when accelerating to high speeds and may experience larger voltage drops. By analyzing voltage levels at different speeds, forensic experts can assess the battery's efficiency at each speed range, which could also reveal if the battery is underperforming or if the drone is operating in a less-efficient power mode.

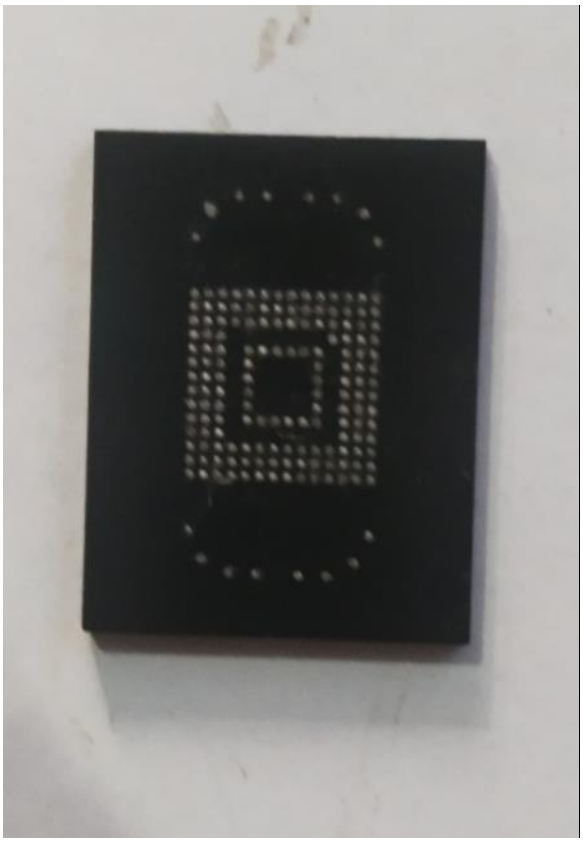
B. Email addresses

Methodology for Forensic Image Acquisition and Data Extraction from Drone Internal EMMC Chip

The forensic analysis of data stored within a drone's internal emmc chip involves several critical steps to ensure data integrity and facilitate subsequent analysis. The process begins by physically removing the emmc chip from the drone. To maintain the integrity of the data and prevent accidental modification, the emmc chip is connected to a laptop using a write blocker, which ensures that no data is written back to the card during the acquisition process.

Step 1: Imaging the emmc chip

The next step is to create a forensic image of the internal emmc chip. For this, we utilized FTK Imager, a widely recognized digital forensics tool. FTK Imager allows for the creation of an exact bit-by-bit copy of the emmc chip, ensuring that all files, including hidden and deleted data, are preserved in their original state. The resulting image is saved for further analysis.

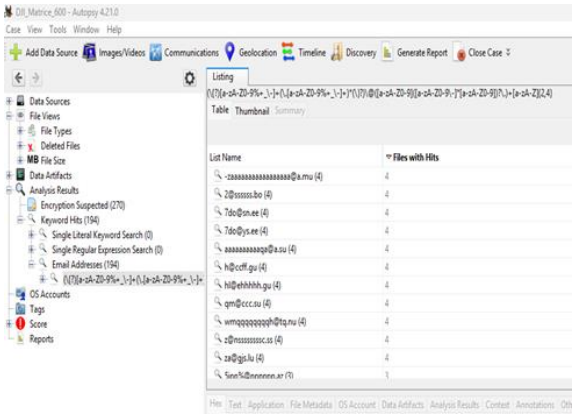


Step 2: Data Analysis with Autopsy

Following the creation of the forensic image, the data from the internal emmc chip is processed using Autopsy (Version 4.21.0). Autopsy is an open-source digital forensics platform that facilitates the examination of disk images, file system analysis, and the extraction of relevant information from a variety of file formats.

Upon analysis, we identified a variety of .dat files stored within the image. These files were subjected to further examination to decode and extract the underlying data. The .dat files contained critical information related to drone operations, communication logs, and potential user data.

Step 3: Extraction of E-mail Communications



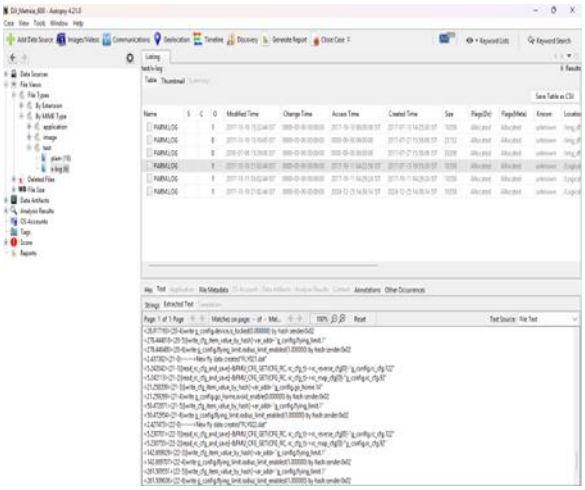
During the analysis, we discovered a total of 194 e-mail records stored within the drone's internal storage. These e-mails included communications from several sources, such as user-generated content, DJI-specific messages, and other potentially relevant communications. This discovery highlights the presence of both user and system data, which could be crucial for investigations involving drone activities, user interactions, and potentially security-related concerns.

C. Drone Log

Forensic Imaging and Analysis of Drone's Internal MicroSD Card

The first step in the forensic examination process is to remove the internal microSD card from the drone. To preserve the integrity of the data, the microSD card is then connected to a laptop using a write blocker, which ensures that no modifications are made to the original data during the analysis.

The next phase involves creating a physical image of the internal microSD card using FTK Imager, a reliable tool for acquiring bit-for-bit copies of storage devices. The microSD card contains several .dat files, which may hold relevant data for further investigation.



Once the image is successfully created, the forensic image of the microSD card is processed using Autopsy (Version 4.21.0), a comprehensive digital forensics platform. Autopsy allows for detailed analysis of the image, including the extraction and decoding of .dat files. During this process, a text file named "cold PARM.log" is discovered. This file contains the drone's event logs, which are critical for understanding the drone's operations, such as flight events, system statuses, and other recorded activities.

This methodical approach enables the recovery of valuable information from the drone's internal storage, providing insights into the drone's activities and aiding in the forensic analysis of the incident.

D. Media We get in Mobile Phone Data in Magnet Axiom Cyber

Forensic Analysis of Mobile Data and Drone-Related Information from microSD Card

This research outlines the forensic methodology for acquiring and analysing data from a mobile device and its associated internal microSD card, particularly focusing on information related to drone operations. The process involves several crucial steps to ensure the preservation of data integrity, followed by the systematic extraction and decoding of relevant files, including data from the DJI mobile application used for drone management.

Step 1: Removal of Internal microSD Card from Mobile Device

The process begins with the physical removal of the internal microSD card from the mobile device. This step is crucial for ensuring that the data on the card remains intact and unaltered. The microSD card is then connected to a laptop using a write blocker, a device that prevents any data from being written back to the card, thereby maintaining its integrity for forensic analysis.

Step 2: Imaging the microSD Card with FTK Imager

Once the write blocker is in place, we proceed to create a forensic image of the internal microSD card using FTK Imager, a widely used tool in digital forensics. FTK Imager is used to create an exact, bit-by-bit copy of the microSD card, preserving all file structures, data, and metadata. This image serves as the foundation for further analysis and ensures that the original data remains unchanged.

Step 3: Extraction of Mobile DJI App Data

Alongside imaging the microSD card, the DJI mobile application data on the device is also extracted. The DJI app is used to interface with drones for control, flight logs, and media management. This data, which can include user settings, flight records, connected devices, and more, is critical for understanding the context in which the drone was operated. The extraction is performed carefully to ensure that all relevant app data, including logs and user configurations, is preserved for analysis.

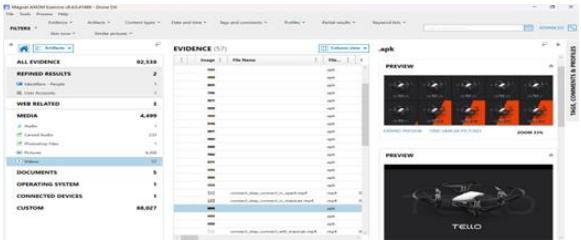
Step 4: Data Processing and Analysis in Magnet AXIOM Cyber (Version 8.4)

Following the acquisition of the forensic image and the extraction of mobile app data, the next step involves processing the data using Magnet AXIOM Cyber (Version 8.4). This powerful digital forensics tool is designed to analyse both mobile device data and external storage, providing a comprehensive view of the extracted information. In this case, Magnet AXIOM is used to process the forensic image of the microSD card and the data retrieved from the DJI mobile app.

Step 5: Extraction of User Data, Connected Devices, and Drone Media

During the analysis, several key pieces of information are retrieved, including:

- User Data: Information related to the user of the mobile device, including preferences, settings, and app interactions.
- Connected Devices: Details of any devices connected to the mobile application, particularly other drones or peripheral equipment.
- Drone Media: Video, images, and other media recorded by the drone during its operation. This includes flight logs, footage, and possibly photos stored within the mobile app or on the microSD card.



E. Forensic Imaging and GPS Data Extraction from Drone's Internal MicroSD Card

1.1 Data Acquisition and Forensic Imaging

The forensic investigation of drone data begins by physically removing the internal microSD card from the drone's on board storage system. This card contains critical data, including flight logs, GPS coordinates, and other operational metadata, which may be essential for reconstructing the drone's flight path and investigating its activities. To ensure the integrity of the data during the forensic examination, the microSD card is connected to a laptop via a write-blocker. A write-blocker is a device that prevents any modifications to the data on the card, ensuring that the original evidence remains unaltered.

Once the microSD card is secured and connected, the next step is to create a forensic image of the card using FTK Imager, a widely recognized digital forensics tool. FTK Imager is used to acquire bit-by-bit copies of storage devices, which is essential for ensuring that the exact contents of the microSD card are captured in their entirety. This imaging process generates a replica of the original data, enabling the investigation to proceed without risking the loss or alteration of evidence. The resulting forensic image, often stored in a standard format (e.g., E01 or DD), serves as the basis for further analysis and is used to maintain an audit trail of the investigation process.

1.2 Processing the Forensic Image and Decoding .dat Files

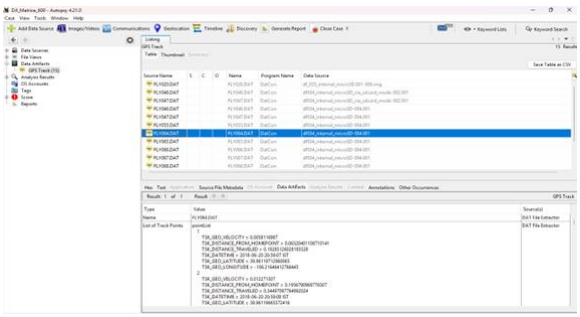
After the forensic image of the microSD card has been created, the next step involves processing this image using specialized digital forensics software. In this case, Autopsy (version 4.21.0) is employed to analyse the contents of the image. Autopsy is a powerful, open-source digital forensics platform that provides a range of investigative tools for the analysis of various types of digital evidence. This software allows investigators to navigate through the data within the forensic image and identify files of interest, including encrypted or proprietary data formats.

Among the files typically found on the microSD card, .dat files are common. These files may contain important drone data, such as flight logs, telemetry information, and GPS coordinates. Autopsy is utilized to decode these .dat files, which may involve extracting structured data from binary formats or decrypting encrypted content. The decoding process is critical for unlocking the information stored within these files, especially when dealing with proprietary data formats used by drone manufacturers. The decoded data provides valuable insights into the drone's operations, including timestamps, flight paths, and geographical locations, which are essential for reconstructing the drone's movements and actions during its flight.

1.3 Extraction and Analysis of GPS Data

Once the .dat files have been decoded, the next step is to extract the GPS data stored within them. GPS data is typically recorded by the drones on board systems during flight, capturing crucial information such as geographic coordinates (latitude, longitude, and altitude), timestamps, and sometimes even specific waypoints or mission parameters. By analysing this GPS data, forensic investigators can reconstruct the drone’s flight path, determining where the drone

operated, its movements over time, and potentially the locations it interacted with.



The GPS data extracted from the forensic image can be visualized using mapping tools or GIS (Geographic Information Systems) software, allowing investigators to generate a detailed visual representation of the drone's flight trajectory. This analysis can be particularly valuable in legal or regulatory investigations, providing concrete evidence of the drone's location history and operational patterns.

In some cases, additional metadata such as flight time, speed, and altitude may also be recovered, offering deeper insights into the drone's behaviour during the flight. By combining GPS data with other flight logs or sensor data, a comprehensive profile of the drone's operational history can be created, which may aid in the investigation of accidents, security incidents, or unauthorized drone activities.

F. Encrypted Drone Data: Overview and How to Decode

Encrypted drone data typically refers to the data that is transmitted or stored by the drone, but secured via encryption methods to prevent unauthorized access or tampering. Drones like the DJI Matrice 300 RTK and others often use encryption to protect various types of data, such as flight logs, telemetry data, video feeds, and location information. This encryption is essential for maintaining security and privacy, particularly in professional and military applications.

Types of Encrypted Drone Data

1. Flight Data Logs: Drones like the DJI Matrice 300 RTK log a variety of flight parameters, including speed, altitude, GPS location, and battery levels. These logs are typically encrypted to prevent tampering, as they are crucial for safety and legal compliance.
2. Telemetric Data: The telemetry data, which includes real-time communication between the drone and the operator (such as control signals, GPS data, and sensor readings), is often encrypted to avoid interception by third parties.
3. Video and Image Data: Some drones encrypt video streams, especially high-definition or infrared imagery, to prevent unauthorized access to sensitive or proprietary content, especially in military or security applications.
4. Mission Planning and Waypoints: Some drones also encrypt mission data, such as predefined flight paths, waypoint coordinates, and geofencing information, to avoid hijacking or misuse of the drone's operation.

Encryption Methods Used in Drone Data

1. AES (Advanced Encryption Standard): Many drones use AES encryption, which is a symmetric encryption algorithm. AES is widely used in consumer and military applications for its strength and efficiency. With AES encryption, both the encryption and decryption processes use the same key.
2. RSA (Rivest-Shamir-Adleman): Some drones might use RSA encryption, especially for tasks involving public-key infrastructure (PKI). RSA is often used in drone communications, especially for the encryption of control messages and secure transmission of sensitive data.
3. TLS (Transport Layer Security): When drones communicate with remote servers or ground control stations, they often use TLS to secure the data over the network. This is especially common when drones are used in cloud-based applications, such as real-time monitoring or fleet management.
4. Proprietary Algorithms: Drones from companies like DJI often use proprietary encryption methods to protect data. DJI, for example, uses a combination of AES and RSA encryption for its drone communications, telemetry, and video feeds.

How to Decode Drone Encrypted Data

- Accessing the Encryption Keys: To decode encrypted drone data, you need to have access to the encryption keys used during the encryption process. If you are the legitimate operator or authorized to access the data, the keys may be

available through the drone's software development kit (SDK) or proprietary tools provided by the manufacturer. For example, DJI provides APIs and SDKs for authorized developers that may allow for access to flight data (with appropriate keys and permissions).

- Using Decryption Software: Once you have the keys, you can use decryption tools to decrypt the data. For AES, tools like OpenSSL or PyCryptodome in Python can be used to decrypt the data. For RSA, you would need to use public-private key pairs, often using libraries like PyCryptodome or Crypto++.
- Accessing Flight Data or Telemetry Logs: In many cases, encrypted flight logs are stored in a proprietary format. For example, DJI drones may store encrypted logs that can only be decrypted using the official DJI software, such as DJI Assistant or DJI Flight Data. These tools ensure that only authorized users can access flight logs, mission data, and other secure information.
- Legal Considerations: It's important to note that attempting to decrypt drone data without proper authorization may be illegal, depending on the jurisdiction. Encryption is implemented to protect privacy and security, and unauthorized decryption or tampering with encrypted drone data can lead to legal consequences.

CONCLUSION

A. Battery voltage drop data provides valuable insights into a drone's speed and power consumption patterns. By examining how voltage fluctuates during different phases of flight, including acceleration, cruising, and deceleration, forensic experts can estimate speed and assess the efficiency of the drone's motors and battery. Combining voltage data with other telemetry readings such as GPS speed or altitude offers a comprehensive understanding of the drone's flight dynamics and can help detect any abnormal behaviours or performance issues related to speed.

B. This methodology illustrates a comprehensive approach to forensic analysis of data stored on a drone's internal microSD card. By utilizing FTK Imager to create a physical image and Autopsy for data examination, we successfully retrieved critical information, including e-mail communications, which may serve as vital evidence in investigations. The ability to extract and decode .dat files further enhances the potential for uncovering additional data stored within the device.

C. The forensic imaging and analysis of a drone's internal microSD card is a crucial method for uncovering valuable operational data. By utilizing tools like FTK Imager and Autopsy, investigators can ensure the integrity of the data while extracting and decoding critical information, such as flight logs and event data. The discovery of files like "cold PARM.log" illustrates the importance of this process in reconstructing a drone's activities. This approach not only supports the effective analysis of drone-related incidents but also enhances the field of drone forensics, offering a reliable framework for future investigations.

D. This methodology outlines a comprehensive forensic approach for analysing mobile device and microSD card data, particularly in relation to drone activities. By utilizing FTK Imager for imaging and Magnet AXIOM Cyber for data processing, we were able to successfully extract and decode critical user and device-related information, as well as media recorded by the drone. This forensic process provides valuable insight into drone operations, user interactions, and device management, which could be essential for further investigation and analysis in a variety of legal and security contexts.

E. By leveraging tools such as FTK Imager and Autopsy, investigators can conduct a thorough forensic analysis of a drone’s internal microSD card. The creation of a forensic image ensures that the original data is preserved, while the subsequent decoding of .dat files and extraction of GPS data facilitates the reconstruction of the drone’s flight path and operational history. This process plays a crucial role in forensic investigations, enabling a detailed understanding of drone activities and providing essential evidence for incident analysis. The use of these methodologies ensures that the investigation remains rigorous, reliable, and legally defensible.

F. Drone data encryption is crucial for maintaining privacy, security, and the integrity of drone operations. DJI, for example, uses encryption

techniques like AES, RSA, and proprietary methods to protect flight logs, telemetry, video feeds, and mission data. To decode encrypted drone data, you typically need the appropriate keys or access permissions, along with decryption software that supports the specific encryption algorithm used. However, it's important to ensure you have proper authorization to access and decrypt any encrypted drone data.

REFERENCES

[1] FTK Imager-

[2] https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81

[3] Autopsy –

[4] https://autopsy.com/download/

[5] MagnetAxiomCyber- https://www.magnetforensics.com/products/magnet-axiom-cyber/

[6] DatCon- https://datfile.net/DatCon/downloads.html

[7] Drone- https://www.dji.com/global/support/product/matrice600-pro

[8] OpenAI