



MONTCLAIR STATE
UNIVERSITY

Montclair State University
**Montclair State University Digital
Commons**

Theses, Dissertations and Culminating Projects

5-2024

Data Recovery Beyond the Obvious Using Digital Forensic Techniques

Smit Chandrakant Nayak

Follow this and additional works at: <https://digitalcommons.montclair.edu/etd>



Part of the [Aviation Commons](#), and the [Information Security Commons](#)

Abstract

Advancement in drone technology, particularly for smaller drones, are creating new research fields and potential applications, particularly with regard to smaller drones. On the other hand, these enhancements bring forth additional hurdles in terms of adaptability, homogeneity, and safety. The purpose of this study is to investigate the science and technology behind drones, as well as their applications, the many ways in which citizens implement them, and the risks, precautions, and privacy problems that are associated with their utilization. This article discusses the existing literature, as well as the available solutions for drone cybersecurity, the security challenges related with drones and data sources, and the existing literature. Although small drones have the potential to assist both the commercial and military sectors, there is still room for improvement in terms of their architecture and security. Internet of Things (IoT) technology has the potential to advance drone technology, but it also raises new worries about privacy and safety. The Internet of Things is seeing exponential growth. To achieve the level of development necessary to fulfill the criteria of the domain, extremely small drones need to be equipped with security, privacy, and data transformation strategies. To conduct digital forensics, we make use of the Autopsy, FTK Imager, and DJI Assistance tools. This allows us to retrieve all flight data that was captured by a drone, including data that has been destroyed. The results of our research can be utilized to develop data recovery procedures for drone forensics that are suitable for any model of drone.

Keywords: - Drone cybersecurity, Autopsy, Digital Forensics, GPS Coordinates, Latitude, Longitude, Flight Path

MONTCLAIR STATE UNIVERSITY

Data Recovery Beyond the Obvious Using Digital Forensic Techniques

By

Smit Chandrakant Nayak

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

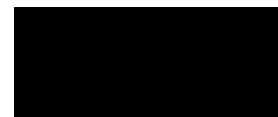
Master of Science in Cyber Security

May 2024

College of Science and Mathematics

School of Computer Science

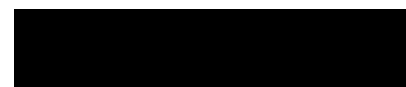
Thesis Committee:



**Dr Bharath Kumar
Samanthula**
Thesis Sponsor



Boxiang Dong
Committee Member



Jiacheng Shang
Committee Member

Data Recovery Beyond the Obvious Using Digital Forensic Techniques

A THESIS

Submitted in partial fulfillment of the requirements

For the degree of **Master of Science in Cyber Security**

By

Smit Chandrakant Nayak

Montclair State University

Montclair, NJ

Graduation Year 2024

Table of Contents

Introduction	1
Drone Characteristics and Features	3
Future Scope	8
Drone Forensic	10
Forensic Case Study	13
Conclusion	45

List of Figures

Figure.1 Statistics for the drone industry	2
Figure.2 Communication Network Types of Drones	3
Figure 3. Types of drones	5
Figure.4 How Attacker Attack On drones	7
Figure.5 Forensic Data Extraction from drones	11
Figure.6 Steps for Creating Forensic Image	14
Figure.7 Selection of Storage Media	15
Figure.8 Selection of Storage Media	15
Figure.9 Selection of Forensics' Image File Type	16
Figure.10 Final Process of Forensics' Image File	17
Figure.11 Completions Process of Forensics' Image File	17
Figure.12 Adding Drone Forensic Image File in Autopsy	19
Figure.13 Selecting Drone Forensic Image File	19
Figure.14 Selecting Drone Data Type	20
Figure.15 Dashboard of Autopsy	21
Figure.16 Captured Information Investigating in Autopsy	22
Figure.17 Flight Records Logs File Information	22
Figure.18 Geolocation Information in Autopsy	23
Figure.19 Image Geolocation Information in Autopsy	23
Figure.20 Flight Log Analysis in Air data	24
Figure.21 Flight Path Analysis	24

Figure.22 Drone Flight Information Analysis	25
Figure.23 Drone Signal Strength Map Information Analysis	26
Figure.24 Drone Altitude Strength Map Information Analysis	26
Figure.25 Captured Photo Video Information Analysis	27
Figure.26 Aircraft log Analysis	27
Figure.27 Aircraft log Analysis	28
Figure.28 Deleted Data Information in Autopsy	29
Figure.29 Deleted Documents Information in Autopsy	29
Figure.30 Deleted Contact Number Recover in Autopsy	30
Figure.31 Deleted Email Information Recover in Autopsy	30
Figure.32 Deleted Drone Flight Log Files Recovery	31
Figure.33 Deleted Drone Flight Log Analysis with Different Location in Air-data	32
Figure.34 Deleted Drone Photo Video Recovery in Autopsy	32

1. INTRODUCTION

Unmanned aerial vehicles (UAVs), commonly referred to as drones, are aircraft capable of autonomous flight or remote control during flight. They are available in a wide range of sizes and shapes. They come in a variety of sizes, ranging from small recreational drones to massive drones used by the military. Drones serve a variety of purposes, including aerial photography and videography, goods transfer, search and rescue missions, and military operations, among others. Recently, there has been significant progress in the underlying technology of drones, leading to increased affordability and accessibility for a broader user base. The rising popularity of drones has led to the creation of new opportunities and applications. Nevertheless, it has also raised fresh apprehensions regarding safety, security, and privacy. The fields of military and defense operations mostly utilize drone technology in today's technologically advanced world. Drones are little aerial machines that function at an altitude of roughly 200 feet above the earth's surface. The technology that supports drones is rapidly evolving with the goal of providing defense.

You can measure the altitude range in feet, meters, or kilometers, depending on the equipment and its intended function. Furthermore, the flight time of these intelligent gadgets may vary based on the specific device. The use of drones in offensive operations is a significant concern for numerous nations and entities, given their potential to transport armaments or explosives as well as conduct reconnaissance and surveillance activities. The use of unmanned aerial vehicles (UAVs) in military operations, as well as their ability to be deployed in acts of terrorism, has prompted a surge in efforts to create counter-UAV technologies and establish legislation to thwart nefarious UAV exploitation. The following are the statistics for the drone industry and its utilization.

- 1) According to forecasts, the worldwide drone market is projected to increase from \$11.2 billion in 2020 to \$43.1 billion by 2025, with a compound annual growth rate (CAGR) of 30.5%.
- 2) The projected period anticipates a Compound Annual Growth Rate (CAGR) of 20.8% for the commercial drone industry.
- 3) The military drone market is projected to experience a Compound Annual Growth Rate (CAGR) of 5.4% throughout the forecast period.
- 4) The civil and commercial drone market is projected to experience a compound annual growth rate (CAGR) of 20.2% throughout the forecast period.
- 5) The agricultural drone market is projected to experience a compound annual growth rate (CAGR) of 23.4% throughout the forecast period.

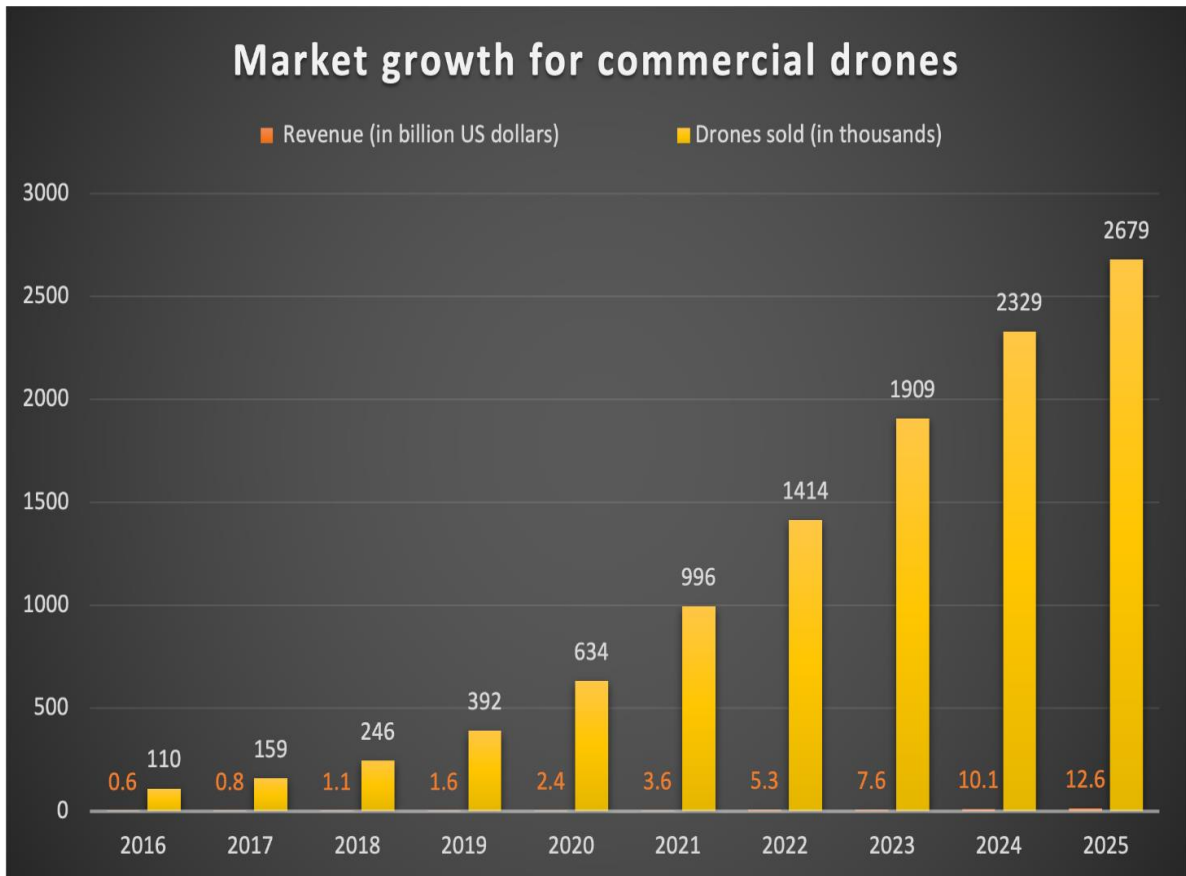


Figure.1 Statistics for the drone industry [1]

Drones have the capability to perform two primary functions: flying and navigating. In order to do these tasks, drones require a power source, such as a battery or fuel, as well as essential components, including rotors, propellers, and a frame. Drone frames frequently use lightweight composite materials to reduce weight and enhance maneuverability.

A controller is essential for the drone's operation. This controller allows the operator to remotely initiate, navigate, and safely bring the aircraft to the ground via remote controls. The controller establishes a connection with the drone by utilizing radio waves, specifically Wi-Fi.

2. DRONE CHARACTERISTICS AND FEATURES

Drone Parts	Drone Features
Flight controller	Cameras
Antenna Maximum	flight time
Battery Media	storage format
Accelerometer sensor	Altitude hold
Ultrasonic sensor	Hover accuracy
Altimeter sensor	Live video feed
Collision avoidance sensors	Sensory range of obstructions
GPS module	Artificial intelligence (AI)
Speed limiters	Augmented reality features
Receiver	Maximum climb and descent rates

Table 1 Typical Drone Characteristics, Parts, and Features

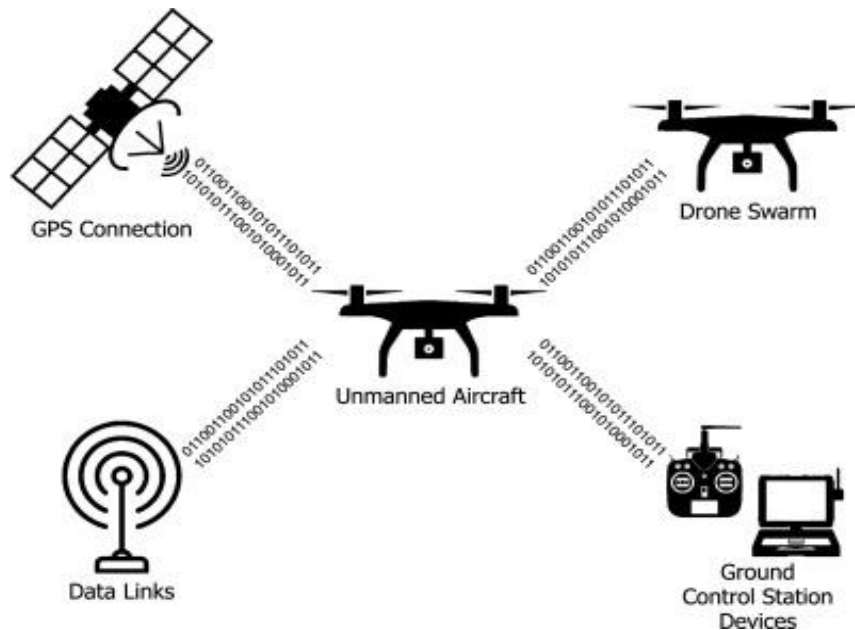


Figure.2 Communication Network Types of Drones [2]

2.1 Drone Feature

A variety of high-performance cameras, including zoom, gimbal steady cam, and tilt, equip the drone. Furthermore, the drone possesses artificial intelligence (AI) capabilities that enable it to track and follow objects. The drone's flight duration dictates its airborne endurance, media storage format, maximum ascending and descending rates, and augmented reality capabilities that overlay virtual objects on its camera feed. Accuracy of hovering. The live video stream provides a sensory range of impediments, while the altitude hold feature maintains a consistent height. The drone possesses flight records and the capability to maintain a consistent height [3].

2.2 Varieties of Drones Have

Multi-rotor drone's the design of multiple rotor and propeller drones allows for vertical takeoff and landing. For those unaware, a drone's propellers can be considered its diminutive wings or blades. These propellers propel the drone through the air, mimicking the flight pattern of a helicopter. The rotor is the mechanism that rotates the propellers. Multi-rotor drones have multiple rotors, whereas helicopters typically have only one. Small to medium-sized drones typically have four rotors, with six and eight being less common. Many rotors can enhance the drone's aerial positioning. The drone's maneuverability improves as the number of rotors it has grows. However, the controls of an 8-rotor drone can be more challenging to comprehend compared to those of a 4-rotor drone. Drones with multiple rotors typically face speed and flight duration constraints due to their lower efficiency compared to other drone types like fixed-wing drones, which can fly continuously for approximately 16 hours. Some multi-rotor drones are incapable of doing large-scale surveys and package delivery because of their limited flight time of about 20 minutes before requiring a battery recharge.

Fixed-wing Drones, equipped with a pair of elongated wings on each side of their main body, require either a catapult or a runway for takeoff. This contrasts with drone models that utilize rotors for flight, allowing them to take off vertically. Furthermore, because of their increased dimensions and heightened challenge in landing, they are unable to hover. Occasionally, military operations use fixed-wing drones for surveillance, but other types of drone flight or aerial photography do not commonly use them. In order to acquire trustworthy photographs and recordings, a drone must possess the capability to hover and maintain flight at precise angles. People commonly use fixed-wing aircraft for recreational purposes or long-distance missions. They do not need to recharge their batteries until they connect new electrical equipment, and they can stay in the air for up to 16 hours continuously. This particular type of drone requires extensive training and expertise in drone piloting, particularly in the areas of takeoff and landing.

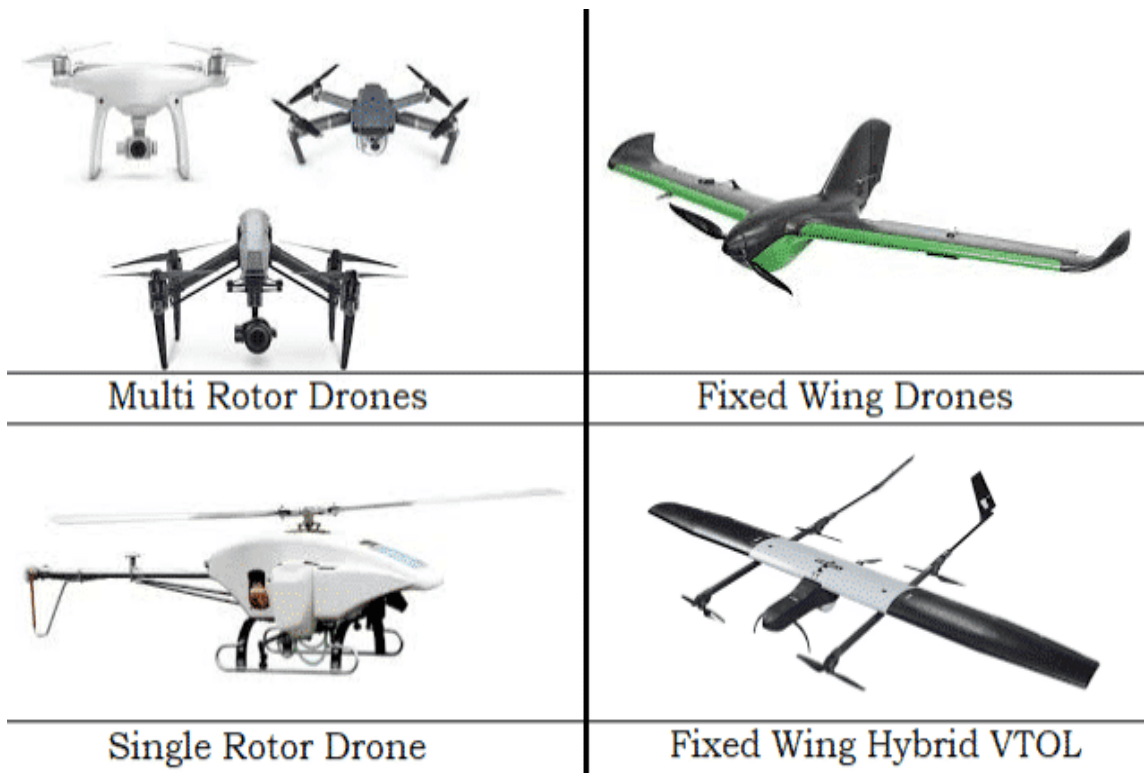


Figure 3. Types of drones [4]

These are unmanned aerial vehicles that use a single rotor for propulsion. Not all helicopters are intended to be large, crewed aircraft. Moreover, manufacturers produce them as smaller, unmanned drones. These drones are available in a broad variety of sizes, ranging from very small toys for children to incredibly large drones equipped with built-in cameras. The price is directly proportional to size. Physical stores sell single-rotor drones for as little as \$20, while online options range in price from a few hundred to several thousand dollars. This professional drone is unique in that, depending on its size, it has the capability to function using gas as a power source instead of electricity. They have lower efficiency compared to fixed-wing drones but higher effectiveness compared to multi-rotor ones. Operating a single-rotor drone can be equally tough as operating a fixed-wing drone, as both require balancing. Hybrid VTOL with fixed-wing configuration This newly developed professional drone combines the vertical takeoff and landing characteristics of a single-rotor or multi-rotor drone with the prolonged flight duration of a fixed-wing drone. Prime Air's drone serves as an excellent exemplification of this concept. VTOL is an acronym that stands for vertical takeoff and landing. However, a drawback of fixed-wing drones is their slower landing speed compared to other drone types, which they compensate for with their significantly longer flight duration. of flight. This combination combines the benefits of both. Despite its very short existence, the concept is slowly acquiring recognition and fame [5].

1. Challenges with drones

1. Endurance Challenge

How: - Hydrogen fuel cell-powered drones have the capability to fly up to three times the distance and for three times the duration compared to aircraft of similar size that are driven by batteries. They operate silently, release just water as emissions, and can be refueled quickly.

Solution: - Fuel cells powered by hydrogen.

2. Navigation Challenge

How: - In the absence of GPS signals, another approach must be employed to ascertain one's location. This little device utilizes a variety of electronic components, all integrated into computer chips, to provide precise information to the navigation system. Equipped with an Inertial Measurement Unit (IMU), the system is capable of accurately determining its precise location, direction, and velocity.

Solution: - Using of Inertial Measurement Unit.

3. Communications Challenge

How: - Maintain communication regardless of your location, whether it is on the opposite side of a hill or thousands of miles apart. SATCOM is the abbreviation for satellite communications. If you are considering using a drone, it is advisable to have the most lightweight and compact SATCOM equipment that is currently available. Users can view real-time video from the drone's cameras and retrieve any supplementary recorded data.

Solution: - Using of SATCOM for small UAVs

4. Detection of Traffic and Obstacles Challenge

How: - A drone must prioritize self-preservation as it lacks the assistance of human visual perception. The drone's primary sensor is its radar. The drone is navigated around other aircraft and obstructions, while simultaneously mapping the area, identifying safe landing zones, detecting its altitude, and even operating in adverse weather. With a length of three kilometers, it could simultaneously monitor multiple objects with great attention.

Solution: - Using IntuVue RDR-84K Radar

2. Drone-based cyber-attacks

A. Disruption of UAV operations (DDOS Attack)

A distributed denial of service (DDOS) attack on an unmanned aerial vehicle (UAV), often known as a drone, is a type of cyberattack that aims to disrupt the drone's operations by overwhelming its network with a high volume of requests. The attack operates by inundating the drone's network with requests originating from one or more sources, with the objective of overwhelming the system and inducing the drone to crash or become unresponsive. These requests can be directed to any element of the drone's network, ranging from the control system to the communications systems. The primary objective of a DDOS attack is to impede the functioning of the drone, leading to its crash or unresponsiveness, hence hindering its ability to accomplish its goal.

B. GPS signal jamming / spoofing

GPS signal jamming/spoofing works by broadcasting a false GPS signal that disrupts or supersedes the authentic GPS signal of the drone. This erroneous signal disrupts the drone's navigation system, hindering its ability to obtain the necessary GPS coordinates for precise location and flight path determination. Consequently, the drone's navigation system will be rendered ineffective, causing it to fail in reaching its intended destination. In addition, the counterfeit signal can be employed to divert the drone, enabling it to be controlled from a distance and directed towards a different location [6].



Figure.4 How Attacker Attack On drones [7]

C. Compromised and misbehaving UAV

A compromised UAV refers to a drone that has been intentionally or unintentionally hacked. This tool has the capability to engage in covert surveillance, launch offensive operations against specific objectives, and carry out acts of espionage or sabotage. The drone can be programmed to autonomously navigate to certain locations and capture photographs or deliver payloads. Furthermore, it has the capability to be programmed to navigate certain regions for the purpose of deploying or managing supplementary unmanned aerial vehicles. Additionally, it can be programmed to disrupt the control systems of other drones or communicate deceptive data to the operator [8].

D. MIT (Man In The Middle Attack)

A Man-in-the-Middle (MITM) attack occurs when a hacker intercepts the data transmitted between the drone and the controller, exploiting it to assume control over the drone. In this type of assault, the assailant has the ability to intercept and manipulate the communications between the drone and its controller, thereby introducing harmful code or making unauthorized modifications. This enables the assailant to assume command of the unmanned aerial vehicle, alter the information it contains, or completely disable it. In addition, the assailant has unrestricted access to all data stored on the drone and can potentially use it to carry out assaults on other systems [9].

3. FUTURE SCOPE

The program to be built must possess a high level of reliability in order to effectively operate with various types of drones. Additionally, it should have the capability to process data in real-time and provide users with precise information. The program should possess the capability to conduct safety verifications and promptly alert the user in the event of any unanticipated data infiltrating the system. To ensure that it store and access data in real-time, the application should have the capability to connect with existing cloud services.

There are three main prospects obtainable in this research observation.

3.1 Anti Forensic Analysis

Drone forensics will soon have a significant impact on the development and implementation of autonomous technologies such as artificial intelligence and robotics. Drones can be utilized to examine and evaluate crime scenes, identify dubious behaviors, and even recreate past events. As AI and robotics grow more prevalent, drones will be capable of providing further understanding of the behavior of both suspects and victims in various situations. In addition, drones may be utilized to examine the digital footprints of suspects and their accomplices, making drone forensics increasingly significant in the investigation of cybercrime.

Drone forensics can be valuable in investigating environmental disasters by utilizing drones to evaluate the effects of an occurrence and provide immediate, up-to-date information.

Drone forensics will be employed to examine occurrences related to national security due of the drones' ability to collect detailed data on suspicious activities and threats. Drone forensics can also be employed to detect and safeguard against potential Distributed Denial of Service (DDoS) attacks that exploit drones as a medium.

3.2 DDOS Attack Implementation

The potential for drone-based DDOS attacks will increase as drones become more advanced. As drone technology advances, drones will possess more data-carrying capabilities and enhanced computing and storage capacities. This will facilitate the utilization of larger, more sophisticated assault vectors. As drone technology advances, it may enable the establishment of networks in previously inaccessible areas, such as isolated or rural locations. Drones can also be employed to launch attacks on networks that utilize advanced and complex protocols, such as mesh networks. Drones can also be utilized to carry out large-scale distributed denial-of-service (DDoS) attacks on many targets. Ultimately, drones can be utilized to execute simultaneous and harmonized assaults on several objectives, as well as launch attacks from various positions. This will empower malicious entities to carry out extensive assaults with reduced likelihood of detection and heightened prospects of achievement.

3.3 Ransomware Attack

There is a possibility that in the future, there may be an increase in the frequency and severity of ransomware attacks carried out using drones. For instance, drones can be employed to gain physical entry into a building and promptly distribute malware to its computer systems. The drones are potentially capable of autonomous flight, enabling them to cover a vast area and potentially engage multiple targets simultaneously. Drones could potentially be utilized to transport and distribute malicious software payloads to vulnerable wireless networks. As attackers get more skilled in operating drones to avoid detection and carry out assaults, the level of complexity in ransomware attacks involving drones may also increase. Attackers could utilize drones to falsify IP addresses, enabling them to carry out undetectable attacks. In addition, assailants have the ability to develop more intricate ransomware payloads that are tailored to certain devices or networks. Ultimately, as drones become more widely accessible, they are expected to be utilized in a greater number of ransomware attacks. The decreasing cost of drones has made them attractive tools for criminals seeking to carry out ransomware attacks. Enterprises must be cognizant of the possible dangers presented by drone-based ransomware attacks and implement measures to safeguard themselves.

4. DRONE FORENSICS

4.1 Drone Forensics

Drone forensics plays a crucial role in the investigations of drone-related crimes conducted by law enforcement and security authorities. It is additionally utilized to examine drone accidents, as well as to identify and discourage illegal drone usage. Drone forensics requires the utilization of specific equipment and procedures. These examples include specialized equipment, software, and knowledge of certain procedures and methodologies. Drone forensics is the retrieval of data from the memory storage of a drone, decoding it, and analyzing it in order to ascertain its source and intended use. This process may need the utilization of specialized software, hardware, and methodologies, such as computer forensics and reverse engineering. The data retrieved from the drone can be utilized to determine the owner of the drone, track its trajectory, and establish the date and time of its usage, among other details. Subsequently, this data can be employed to reconstruct the events and establish a legal case against the alleged perpetrator [10].

4.2 What information extracted from drone?

A skilled cyber forensic data analyst is capable of recovering deleted files and investigating the interaction between the drone and the server it exchanges data with. Through the application of drone forensics, we are able to uncover more evidence, which may include the following artifacts:

- WIFI, IP, Bluetooth, 3G and 4G connection Information.
- Input from the pilot, settings made by the pilot, and the firmware version.
- Dates and timestamps for photographs, movies, and geolocations.
- GPS status when flying, the serial number of the drone and internal components (MAC, SSID, and IMEI).
- Atmospheric conditions experienced during each stage of the journey, In addition, the digital forensics investigation may uncover many technical details, such as the altitude of the device at each location and the pace at which it was traveling.
- Places for takeoff, landing, returning, and returning base station (includes popular and favored flying locations).
- Pictures shot; videos recorded by drone operator.
- History of flights, including precise locations and routes taken.
- Storage types and size information.
- Logs of protected zone activity, as well as flight plans and objectives.
- Device Information which use as a remote controller for drones like IOS or Android.
- Sensors information such as controllers, gyroscopes, accelerometers and barometer avoidance and ultrasonic sensors.

4.3 Types of Drone Forensics

In digital forensics, we have basic two type of forensic data extractions methodology which is following.

a. Logical Data Extractions: -

Logical Data Extractions All data is extracted directly from the source system at once.

b. Physical Data Extractions: -

Physical Data Extraction Source systems often have certain restrictions or limitations. For Ex, drawing data from outdated data storage systems via logical extraction is impossible. The data can be extracted only by Physical Extractions [11].

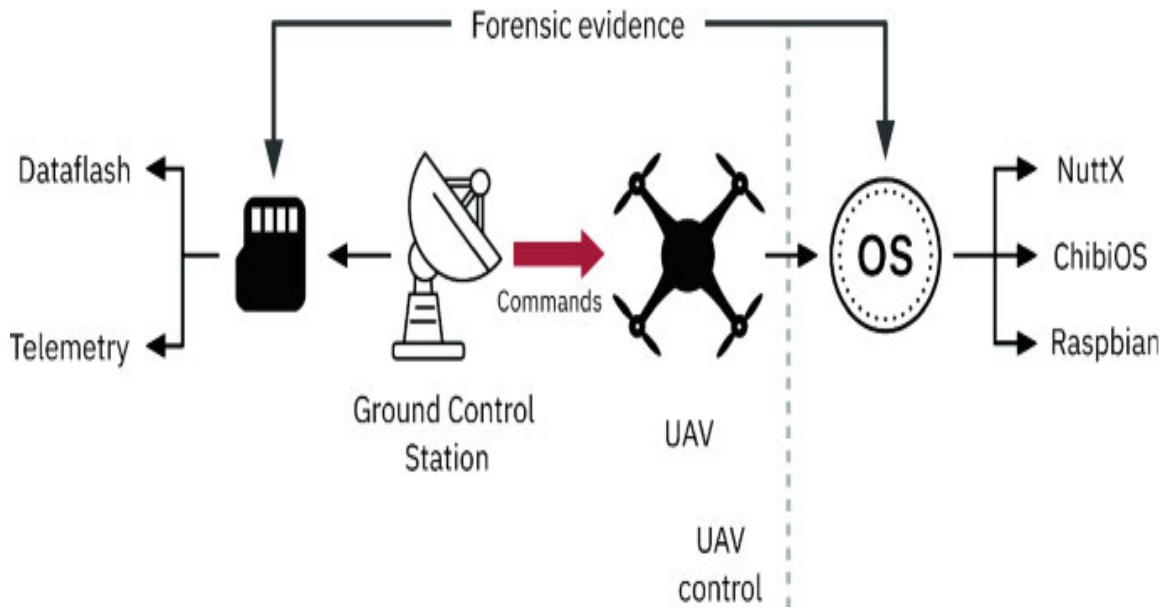


Figure.5 Forensic Data Extraction from drones [5]

The complete drone forensics process can be divided into five stages which is following is

1) Physical Forensics: -

The actual components of the drone, such as the camera, flight controller, motors, and other hardware, are the focus of this sort of drone forensics.

2) Digital Forensics: -

The data recorded on the drone's memory card, such as flight logs, images, and movies, is examined in this sort of drone forensics. This forensics technique can also be used to recover deleted data.

3) Radio Frequency Forensics: -

This sort of drone forensics focuses on the drone's radio frequency signals, such as the GPS signal, Wi-Fi signal, and Bluetooth signal. This form of forensics can also be utilized to study the flight path of the drone.

4) Network Forensics: -

This branch of drone forensics examines the routes of communication that the drone employs to speak with its controller and other surrounding gadgets.

5) Environmental Forensics: -

This branch of drone forensics examines the drone's surroundings, including the topography, wind speed, and other elements that may affect the drone's performance.

5. FORENSIC CASE STUDY

The first step is to establish a connection between the drone, remote control, and smartphone. Both the drone and the smartphone underwent factory reset processes. Utilizing the DJI Mini 2 SE software, we performed a formatting operation on the drone's internal storage. We restored the drone to its original factory settings and updated the firmware using the same application, following the removal of all non-volatile files from the internal storage. Prior to receiving the most recent operating system update, the iOS device was restored to its original factory settings, and the Android phone underwent a similar restoration to its factory settings before acquiring the latest firmware along with the most recent security patch [12].

This project's major purpose is to save, acquire, examine, and analyze drone data. Table 2 illustrates the focus of the research instruments in this work, which is on the drone and its mobile platform. Android was picked as the mobile platform alongside the iOS platform due to its market dominance.

TOOLS	Descriptions
DJI MINI SE 2	Battery Capacity 2250 MAH, Storage 32GB Samsung External Memory Card, Sensing Precise Hovering Range: 0.5-10 m, Remote Controller DJI RC-N1 Remote Controller, 3-axis mechanical gimbal (tilt, roll, and pan), Camera 1/2.3-inch CMOS, Effective Pixels: 12 MP 2.7K: 3x FHD: 4x Digital Zoom.
DJI Assistant	This can be used to obtain data from a DJI drone, as well as to parse retrieved flight records into CSV files.
I Phone 13 Pro Max	IOS 16.5, Storage 256 Gb used as base Controller of DJI Mini Se 2 drone.
Autopsy	An end-to-end open-source digital forensics platform built by Basis Technology, with most features available in other commercial forensics tools. The tool was able to recognize the file system structure, recorded media files, timeline, display Exif data, system files, and thumbnails (displayed in a visually organized way).
FTK Imager	Access Data created a data preview and forensic imaging tool.
Air Data UAV	This utility is used to analyze flight log files.

Table.2 Hardware and Software's Used

Drone Forensic Image Creations Steps

In this study, I utilized FTK Forensic Imager to produce forensic image files from any digital storage device such as a memory card, hard disk, SSD, or Pen drive.

5.1 FTK Imager

FTK Imager is a freely available software application created by Access Data. Its purpose is to generate precise duplicates of original evidence without making any changes to it. The original evidence image stays unaltered, enabling us to duplicate data at a much-accelerated pace, facilitating swift storage and subsequent evaluation.

The FTK imager additionally has an integrity testing function that creates a hash report that aids in comparing the hash of the evidence before and after making the image of the original Evidence. One of the most important phases in digital forensic inquiry is forensic imaging. It is the process of creating a backup or archival copy of the complete hard disk. It is a storage file that contains all of the information required to start the operating system. However, in order for this imaged disk to operate, it must be applied to the hard drive. The disk image files cannot be used to recover a hard drive since they must be opened and loaded on the drive using an imaging application. Many disk images can be stored on a single hard drive. Disk images can also be saved on bigger capacity flash devices [13].

5.2 Making a Forensic Image of A Drone Memory Card.

After installing FTK Imager by Access Data, you will have to insert the storage media which you want to make the forensic image after that following steps are mentioned. for creating a drone external memory card forensic image.

Steps: - 1 To make a Disk Image, use the Create Disk Image command. Select File, Click on Create Disk Image.

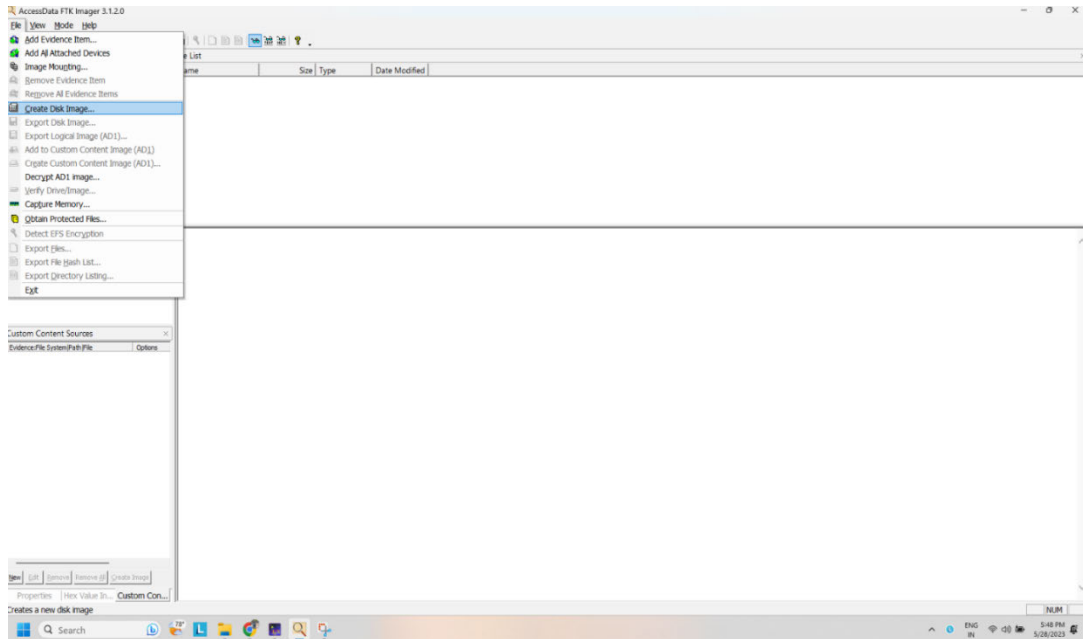


Figure.6 Steps for Creating Forensic Image.

Steps: - 2 You can now select the source based on the drive you have. Depending on the size of your evidence storage, it can be a physical or logical drive.

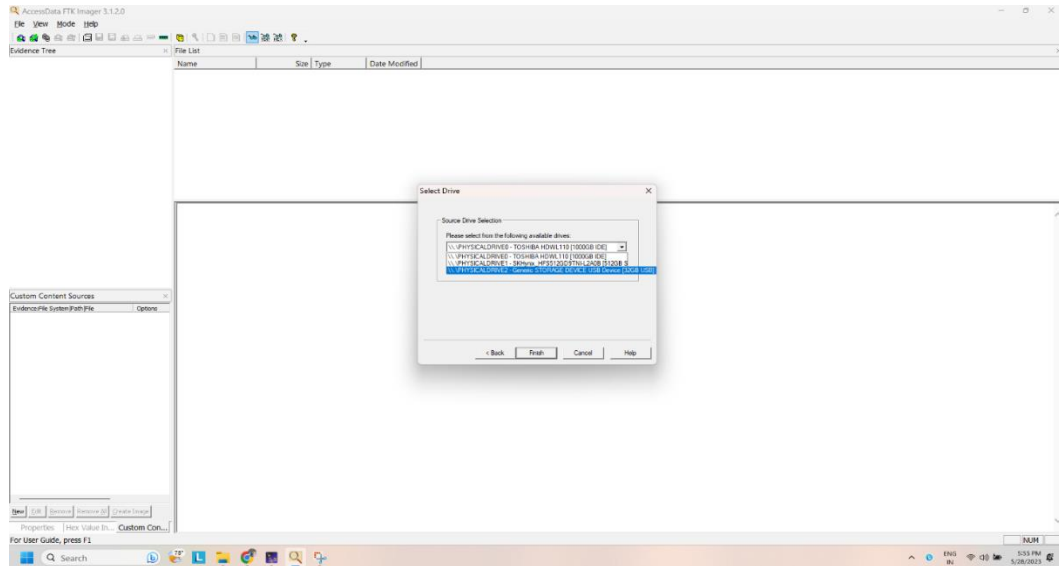


Figure.7 Selection of Storage Media

Steps: - 3 Fill in the Destination path for the image that will be created. To prevent evidence loss, it should be copied in a different hard drive and several copies of the original evidence should be generated.

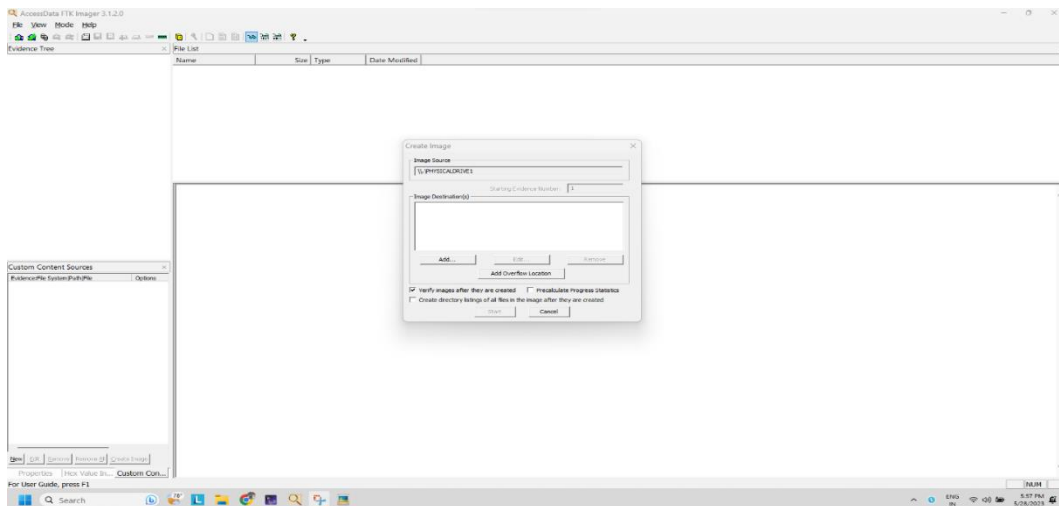


Figure.8 Selection of Storage Media

Steps: - 4 Choose the image format that you want to create. The image can be created in the following formats.

- ✓ **Raw(dd):-** It is a bit-by-bit replica of the original evidence, with no additions or omissions. They are devoid of metadata.
- ✓ **SMART: -** It is an image format used for Linux that is no longer widely used.
- ✓ **E01 :-** It stands for EnCase Evidence File, which is a typical image format that is related to.

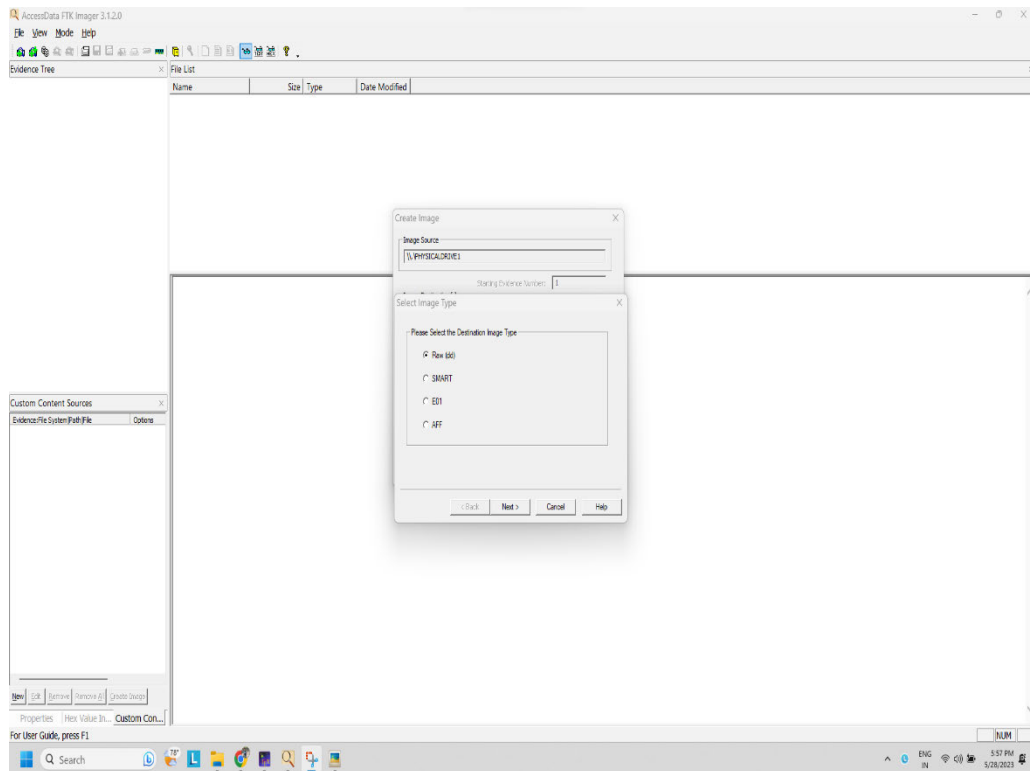


Figure.9 Selection of Forensics' Image File Type

Steps: - 5 Finally, add the forensic images file's location, name the image file, and then click Finish. After you've entered the destination directory, you can begin with the Imaging and also select the Verify option to build a hash.

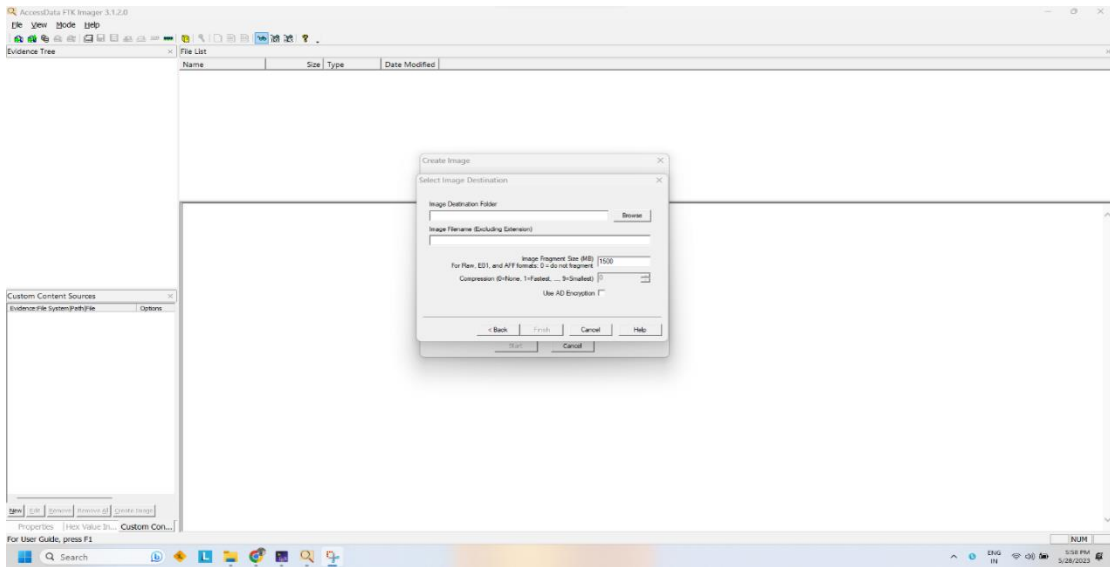


Figure.10 Final Process of Forensics' Image File

Steps :- 6 Following the creation of the image, a Hash result is obtained that confirms the MD5 Hash, SHA1 Hash, and the presence of any faulty sectors.

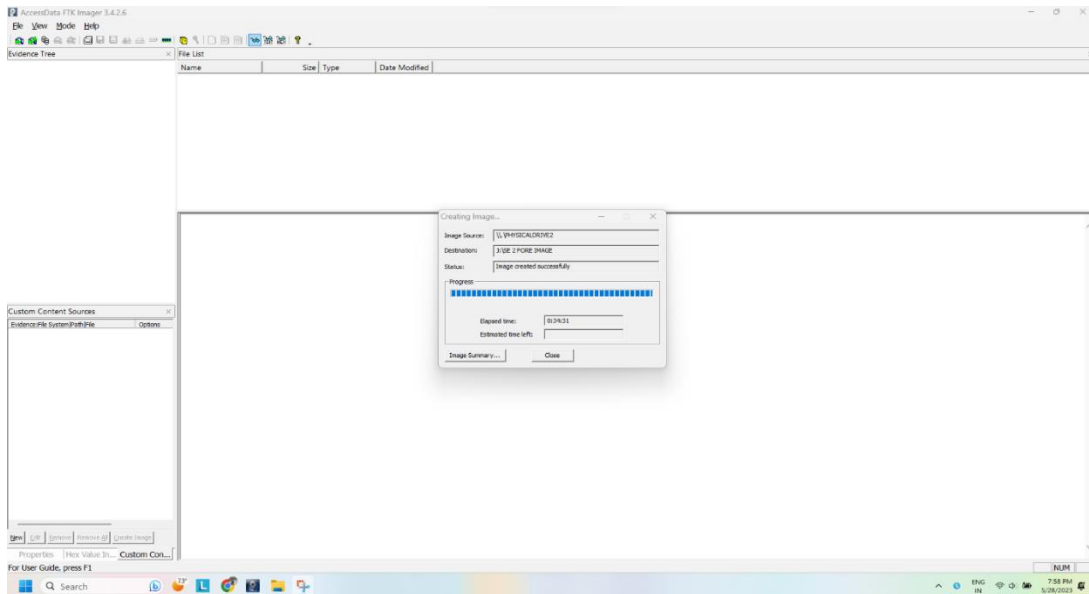


Figure.11 Completions Process of Forensics' Image File

After we have completed the drone external memory card forensic picture procedure, we must open that image in Autopsy Forensic software, which are open source software that can be simply downloaded from the internet.

5.3 Autopsy Overview

Autopsy is a platform for digital forensics that provides a graphical user interface for various digital forensic tools, such as the Sleuth Kit. For examining what transpired on a computer, law enforcement, the military, and corporate examiners utilize this technology. It is even possible to recover photographs that have been deleted from a flash drive or memory card. Autopsy's user interface has been designed to be intuitive right out of the box. A wizard will guide you through the installation process, which is rather basic. There is just one path that leads to all the findings, and that is the main branch [12].

Autopsy was designed to be an all-inclusive platform with modules that come pre-installed on the system and others that can be purchased separately from third-party developers. Autopsy modules contain the below-mentioned features.

Hash Filtering: - Mark known malicious files and disregard known good files.

Timeline Analysis: - Interface for advanced graphical event viewing for drones.

Keyword Search: - Indexed keyword search to locate documents that include pertinent terms.

Web Artifacts: - Extract the browser's history, bookmarks, downloaded data information and cookies.

Data Carving: - Retrieve deleted files from free space.

Autopsy hashes all files, unpacks standard archives (ZIP, JAR, etc.), extracts any EXIF values, and indexes keywords in major file systems (NTFS, FAT, ExFAT, HFS, Ext2/Ext3/Ext4, YAFFS2). Some file types, such as conventional email formats and contact files, are processed, and catalogued as well. Users can browse these indexed files for recent activity or generate an HTML or PDF report that summarizes relevant recent actions. If time is of the essence, users can enable triage features, which utilize rules to evaluate the most important files first. The autopsy can store a portion of these files in a VHD image [14].

After creating a forensic image of the drone memory card, we must open that image file in the autopsy forensic program. The steps and screenshot below show the whole forensic data recovery procedure that we employ to obtain information from the drone.

Steps: - 1 Start the Autopsy tool and select the Make a New Case after that Add the case number and examiner's name, then select your forensic virtual machine or hard disk image file.

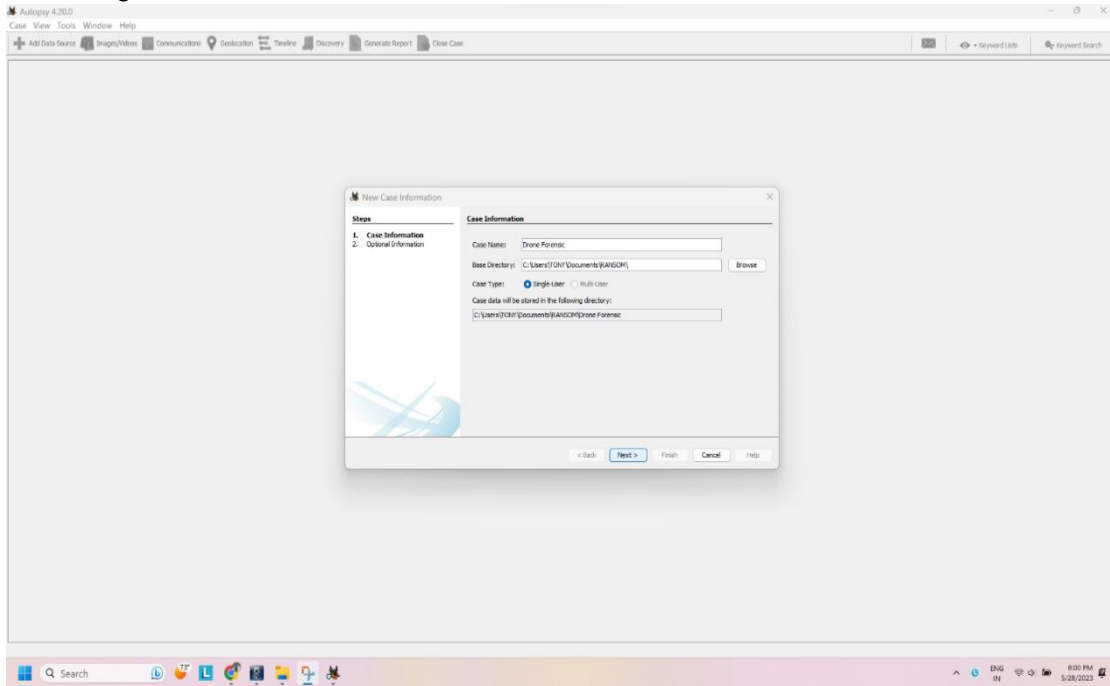


Figure.12 Adding Drone Forensic Image File in Autopsy

Steps: - 2 Select a Data Source (Forensic Image) File for Forensic Analysis.

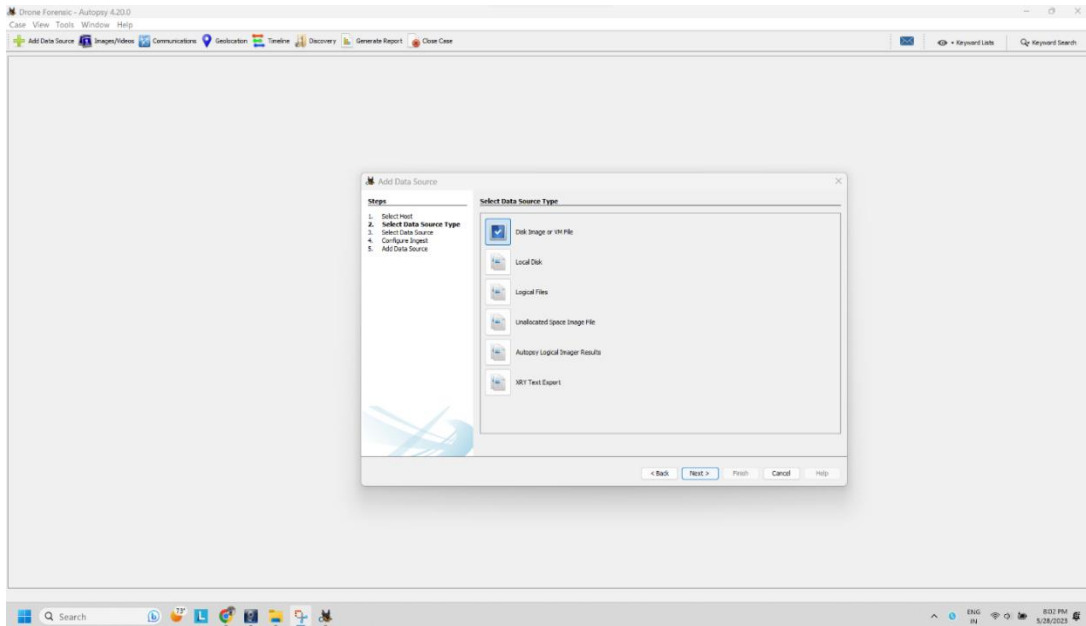


Figure.13 Selecting Drone Forensic Image File

Steps: - 3 Click on configure ingest option and select DJI Drone Analyzer.

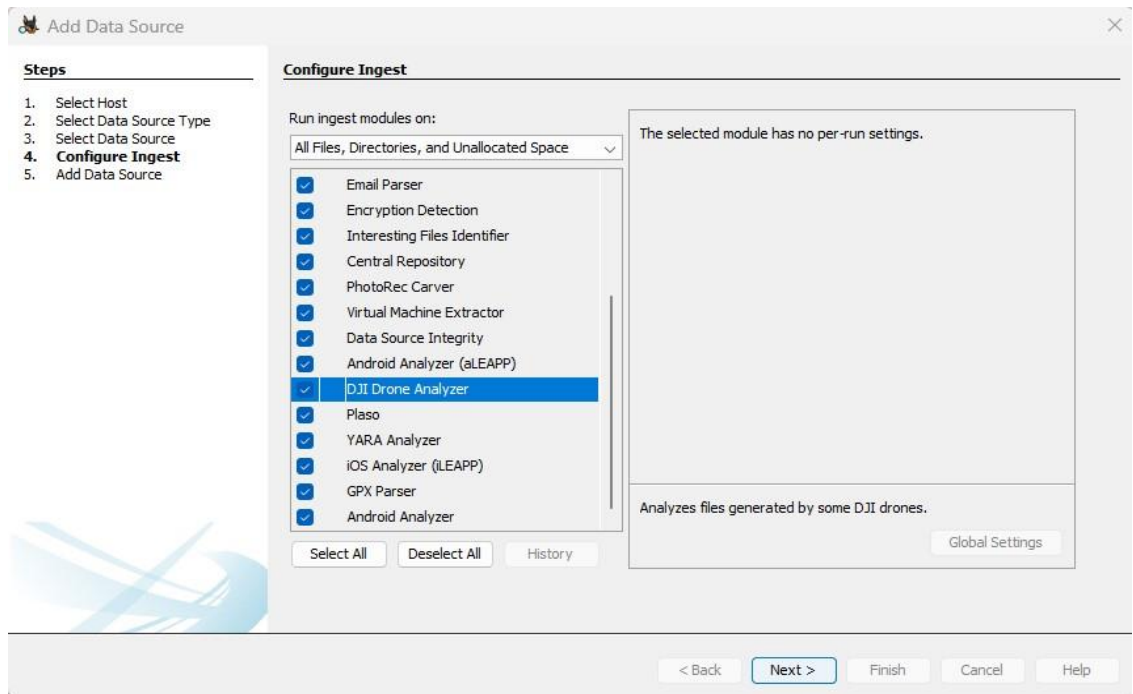


Figure.14 Selecting Drone Data Type

After completing the loading procedure of the forensic image file, we were able to obtain much information such as flight logs, recorded images and videos, and even deleted data from that memory card, which is already used in the Android device for data storage. following information recovered successfully from the drone SD card.

File Type	Number of Files	Formats
Images	7953	JPEG, PNG, GIF, BMP, TIFF, etc.
Video	388	MP4, AVI.
Audio	799	MP3
Documents	162	PDF, Word, Excel, etc.

Table.3 Total Number of Files Recovered from SD Card

Throughout this study, we have acquired a substantial volume of data from the drone's SD card, which can serve as authentic digital evidence for any cyber-crime. Below, you can find information and specifics about the investigation of drones for forensic purposes.

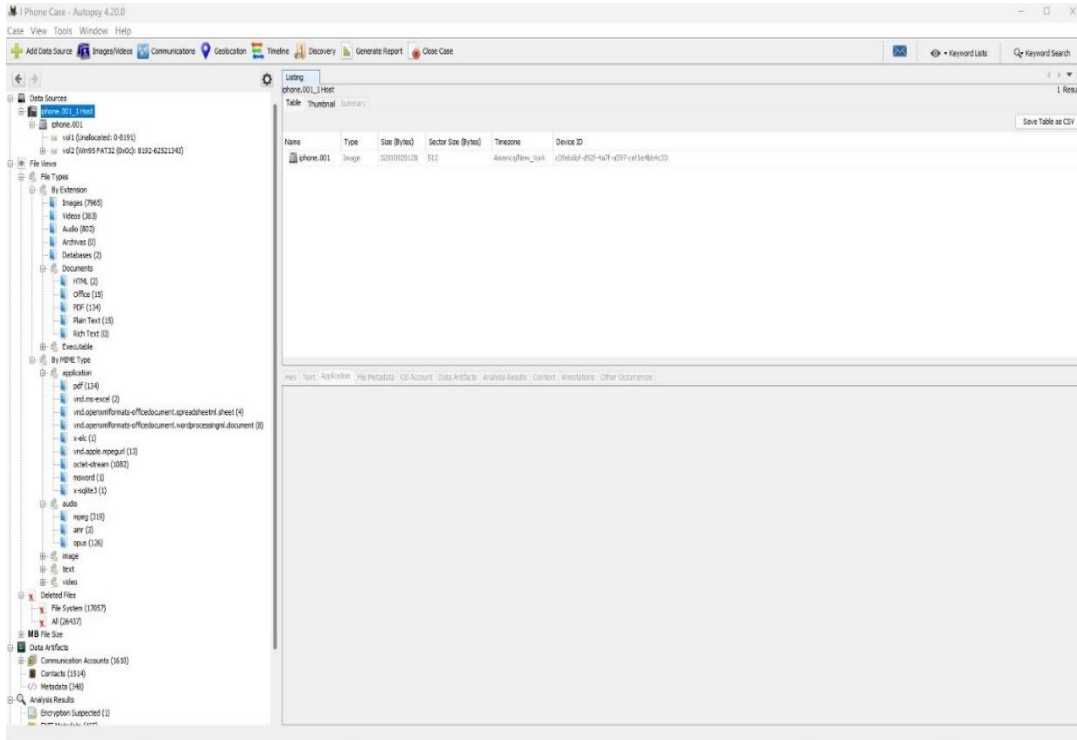


Figure.15 Dashboard of Autopsy

1. **Capture Photo and Videos:** - In this investigation, we discovered images and videos captured from the drone. The image clearly shows that the photo and video were captured in the evening time, and we can see the date and time for this information was captured by the drone, so technically all information is clicked on **2023-06-01**, evening time at **20:30:29 pm**.

We may view the latitude (**40.45627675**), longitude (**-74.4990005555556**), altitude (**39.729**), and device model information during an autopsy, which can be used as lead information for forensic inquiry.

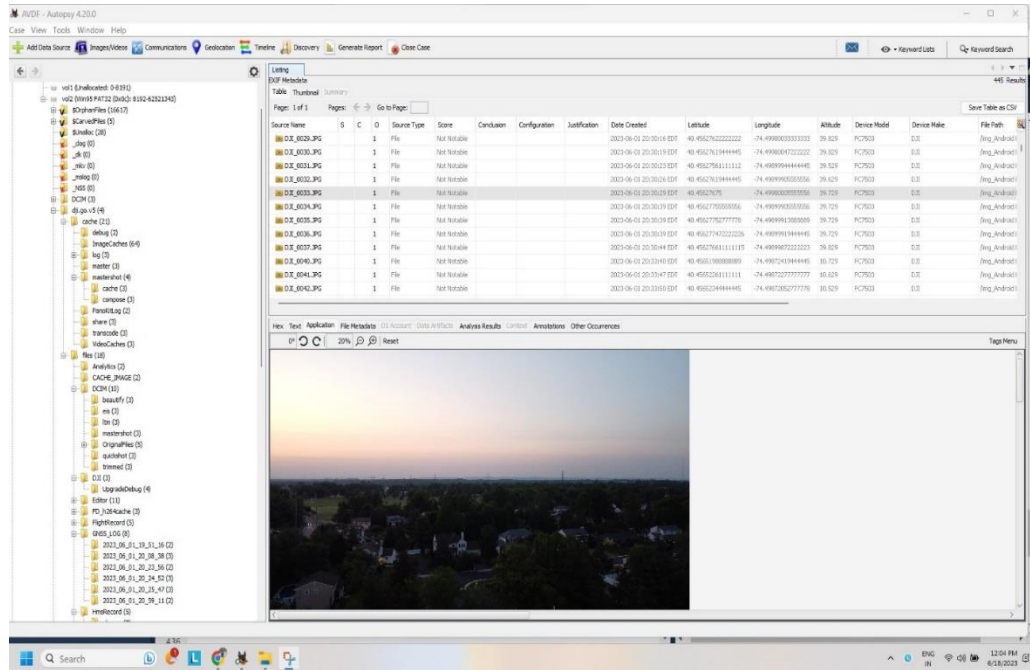


Figure.16 Captured Information Investigating in Autopsy

2. **Flight Records Logs:** - Drone forensic flight record logs file plays the most significant part in an investigation where we can retrieve information regarding the true location of crime viewed and aid to gain leads in cybercrime cases.

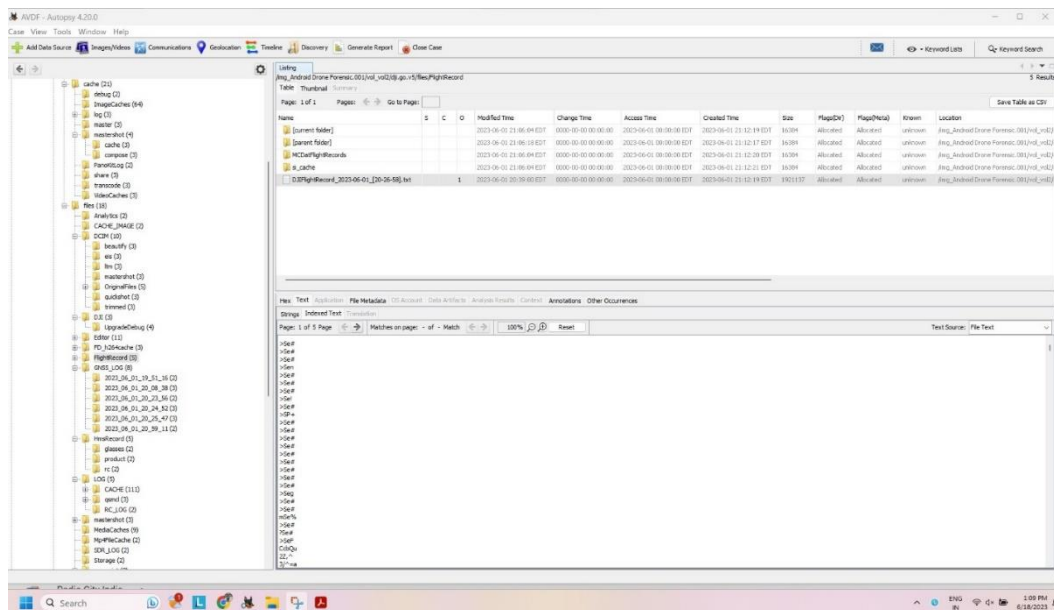


Figure.17 Flight Records Logs File Information

I use the Geolocation editor function after extracting the flight log file into the autopsy. It helps to supply information on the device real location which we found at the crime scene.

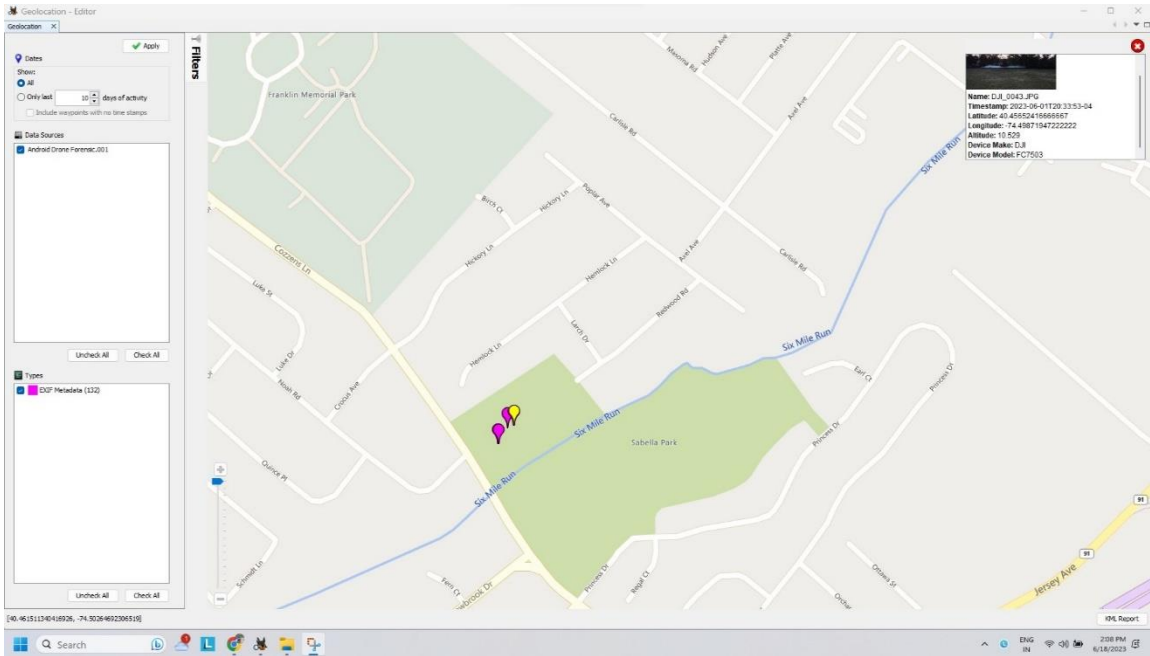


Figure.18 Geolocation Information in Autopsy

In Geolocation Editor are able to retrieve information particular image information like time stamps (**2023-06-01**), Time (**20:33:53-04**), Latitude (**40.4565241666667**), Longitude (**-74.49871947222222**), Altitude (**10.529**), Device Make: - DJI, Model Number: - **FC7503**.

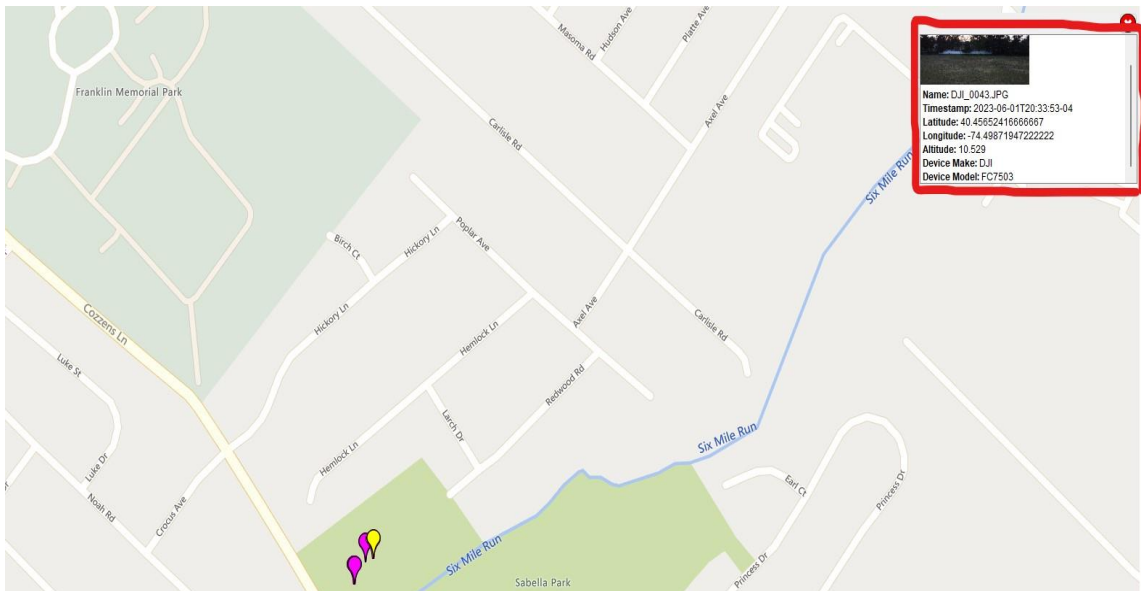


Figure.19 Image Geolocation Information in Autopsy

Now that we have more genuine and accurate information and a location for that specific drone, I used the air data web application and the phantom help application to analyze drone log files. which provides more detailed information on the drone and open-source tools. The graphic above provides exact information about the drone's location, flight time, data, and duration of the flight, which is 100 per cent correct and accurate.


Metric / Imperial Settings	Overview	Details	Equipment	Notifications	Large Map	🗑️	🔄
GENERAL	Associated Pilots:	Tony Patel PILOT-IN-COMMAND					United States
POWER	Take Off Location:	40.456493,-74.498831 Above Sea Level: 99.0 ft					
SENSORS	Address:	1451 Cozzens Ln, North Brunswick Township, NJ 08902, USA Edit Address					
CONTROLS	Last Known Location:	40.456493,-74.498837 at log time of 12m 01s and altitude of -3.3 ft					
WEATHER	Log Duration:	12m 01s (time in the air and on the ground)					
	Air Duration:	11m 59s (time in the air only)					
MEDIA							

Figure.20 Flight Log Analysis in Air data

The graphic above depicts the Drone's flight path; the green highlighted line represents the entire flight path. The blue mark indicates the drone's battery condition during flight, and it continues to decrease, indicating that the drone flew for more than 5 minutes in the same place to capture the information regarding the crime spot.

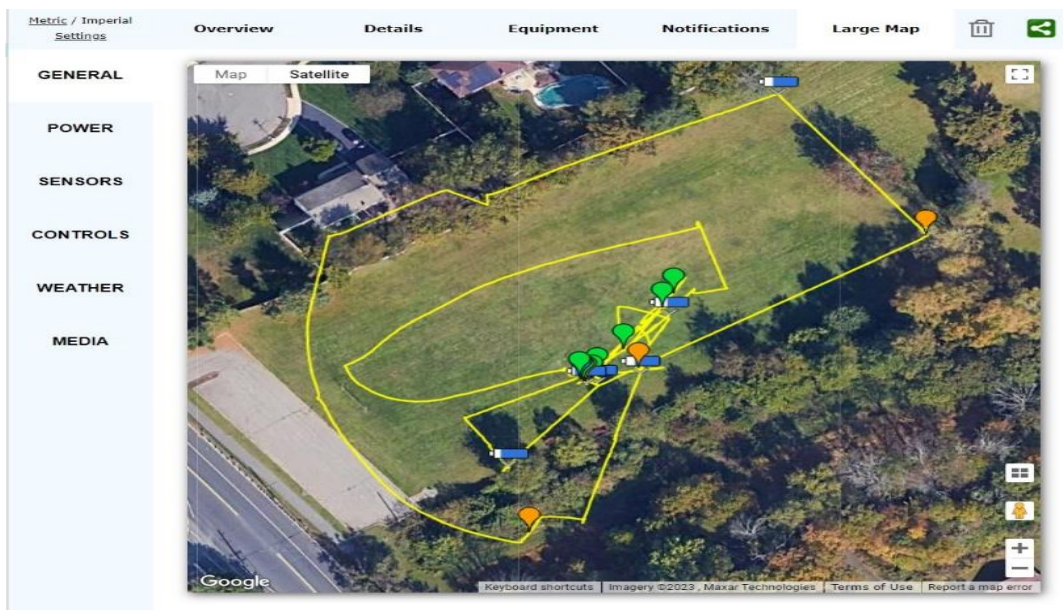


Figure.21 Flight Path Analysis

Furthermore, the green balloon icon represents the safe altitude, while the orange balloon icon represents the highest capacity altitude during the flight. The image above illustrates the Drone's flight parameters, including flight duration **11m59s** time and date, Minimum flight height **133.5 FT**, Maximum flight height **284 FT**, battery percentage information during takeoff (**93%**) and landing (**49%**), weather information, and wind speed **17.40mph**, including captured photo information.

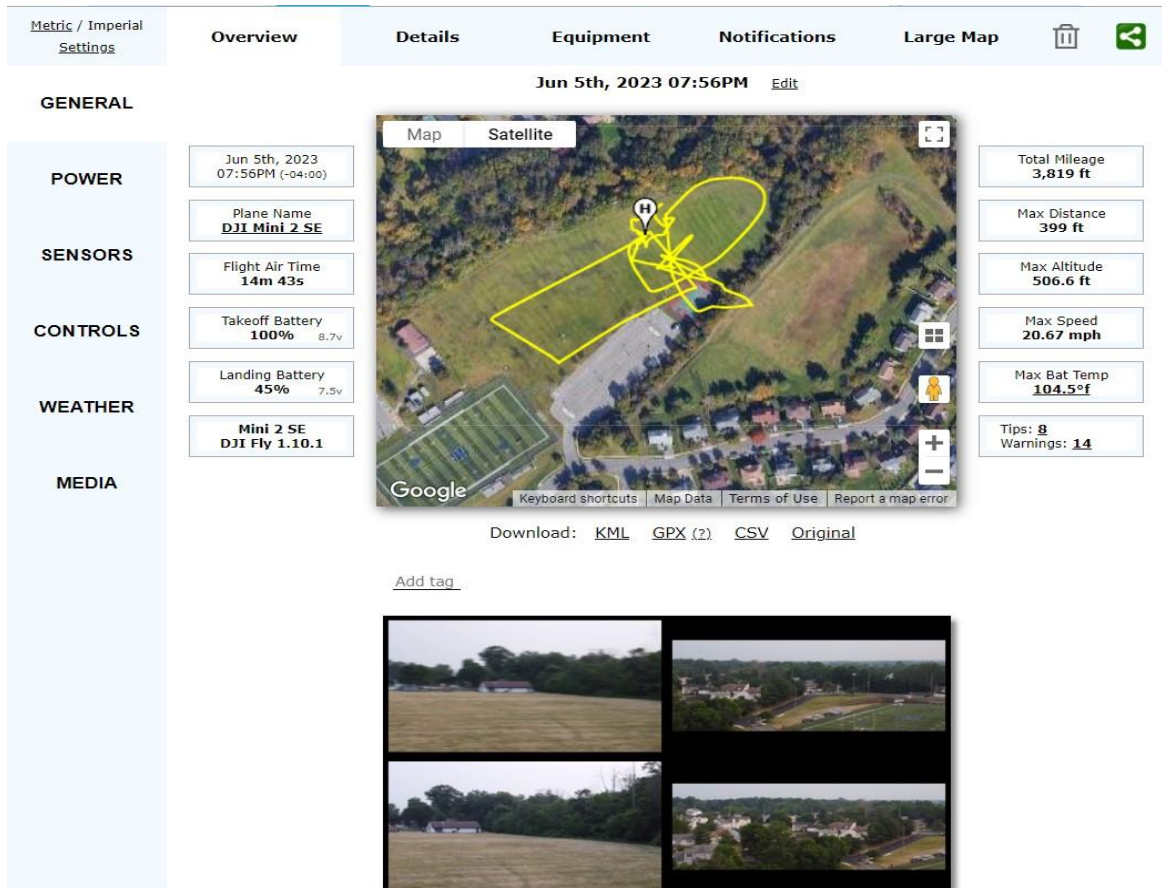


Figure.22 Drone Flight Information Analysis

I discovered vital information on drone signal strength in this study. Signal strength is critical since it leads to the closest position of a cybercriminal, and it is then very easy to locate the drone's base station.

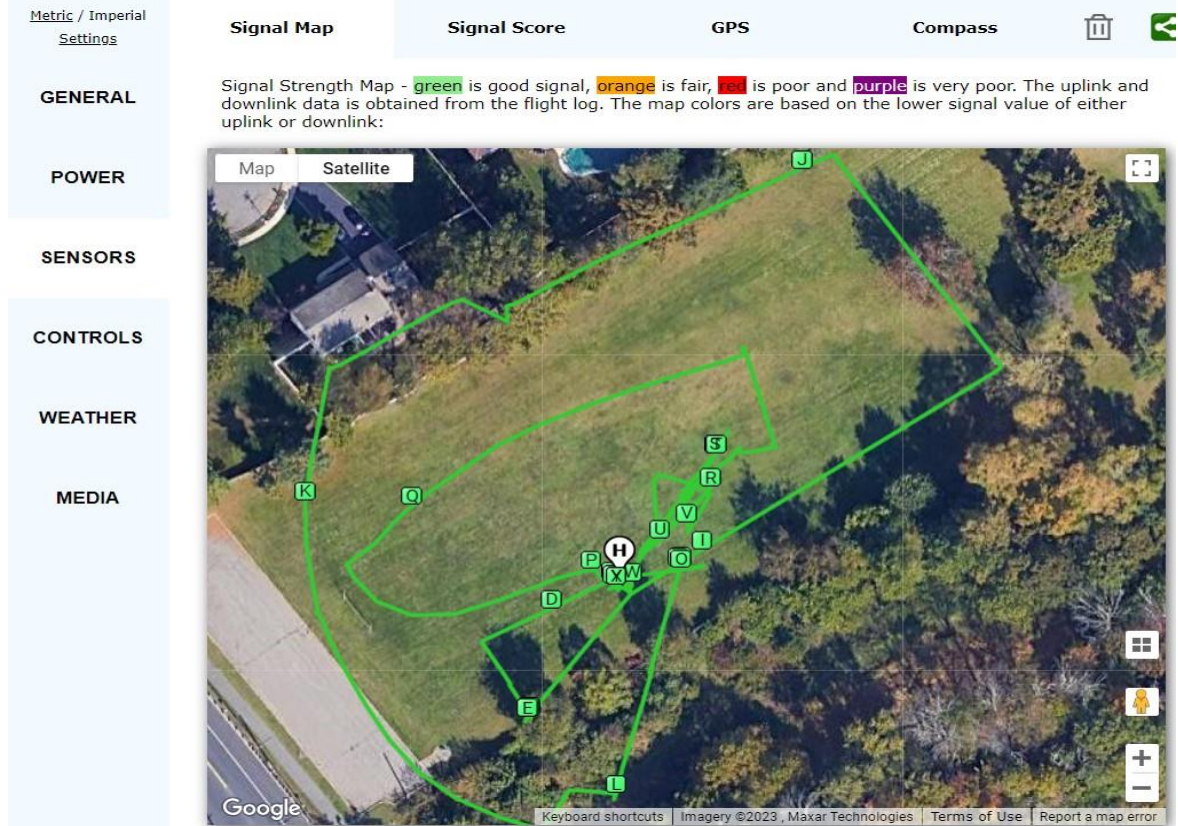


Figure.23 Drone Signal Strength Map Information Analysis

This figure depicts a signal intensity map with flight time and heights. up-links is used in drone and down-link is used by the remote controller to receive the signal.

	Flight time	Altitude	Home Distance	Uplink Signal	Downlink Signal
A	00m_30s	7.2 ft	2 ft	98%	99%
B	01m_00s	6.2 ft	3 ft	100%	100%
C	01m_30s	49.5 ft	4 ft	100%	100%
D	02m_00s	67.3 ft	38 ft	100%	100%
E	02m_30s	74.1 ft	93 ft	100%	100%
F	03m_00s	112.2 ft	92 ft	100%	100%
G	03m_30s	109.9 ft	92 ft	100%	100%
H	04m_00s	109.9 ft	92 ft	100%	100%
I	04m_30s	109.6 ft	49 ft	100%	100%
J	05m_00s	109.3 ft	270 ft	100%	100%
K	05m_30s	109.9 ft	174 ft	100%	100%
L	06m_00s	114.5 ft	126 ft	100%	100%
M	06m_30s	15.4 ft	35 ft	100%	100%
N	07m_00s	13.8 ft	33 ft	100%	100%
O	07m_30s	3.9 ft	35 ft	100%	100%
P	08m_00s	94.8 ft	18 ft	100%	100%
Q	08m_30s	72.2 ft	120 ft	100%	100%
R	09m_00s	53.5 ft	77 ft	100%	100%
S	09m_30s	25.6 ft	95 ft	100%	100%
T	10m_00s	102.0 ft	95 ft	100%	100%
U	10m_30s	5.2 ft	36 ft	100%	100%
V	11m_00s	2.6 ft	52 ft	100%	100%
W	11m_30s	3.3 ft	7 ft	100%	100%
X	12m_00s	-1.6 ft	2 ft	100%	100%
Y	12m_01s	0.0 ft	2 ft	100%	100%

Figure.24 Drone Altitude Strength Map Information Analysis

Air data allows you to view photos taken by the drone from the same log file from which we may recover information.

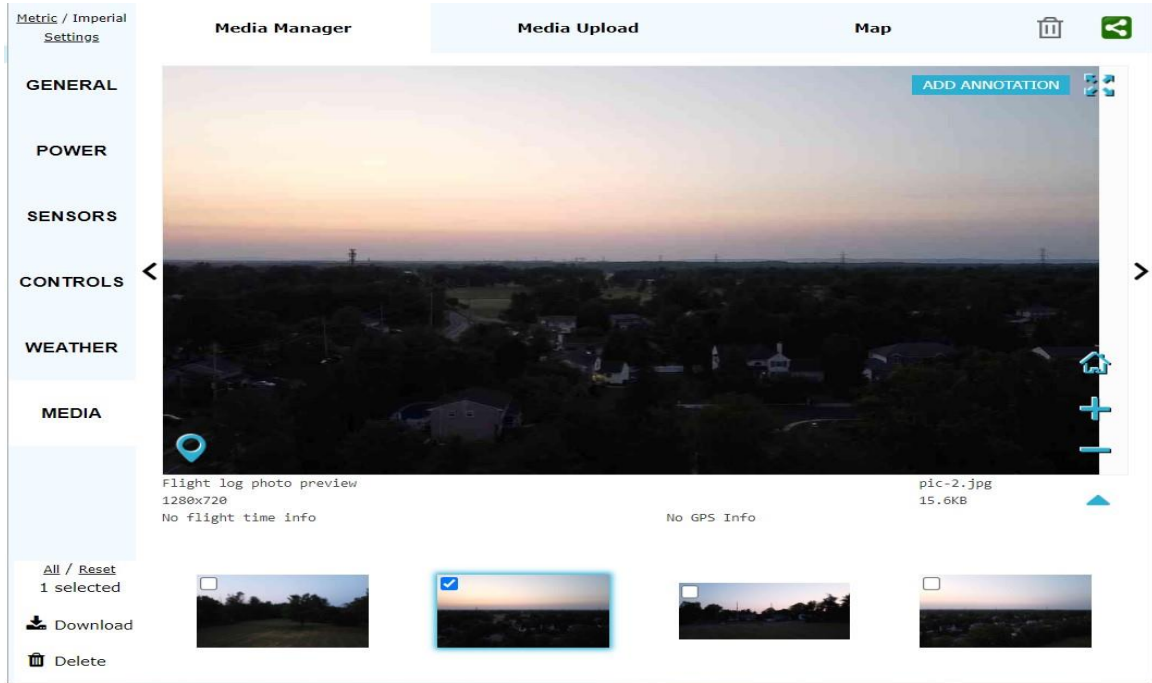


Figure.25 Captured Photo Video Information Analysis

Analysis of aircraft logs It is more essential in drone forensics since it provides more technical information about drone flight. I utilized an open-source tool called Flight Reader for DJI drones to analyze aircraft logs. The image displays information about the exact time, location, height, batteries, and speed. The red circles indicate that the drone is stable in the air during the flight.

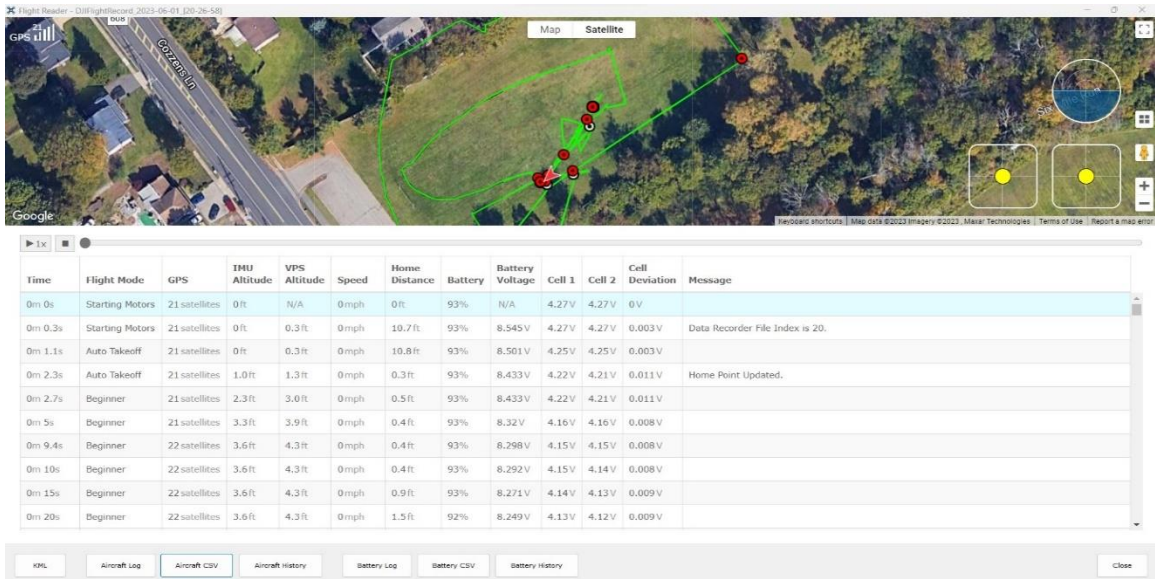


Figure.26 Aircraft log Analysis

In the detailed analysis of Aircraft Log Analysis, I was able to obtain more information about the aircraft take-off and landing operation. It provides detailed information every second. In this scenario, the drone is flying for more than 11 minutes in the air, and the battery level and altitude level values are changing every second.

The screenshot shows a flight log analysis window with a table of data. The table has 13 columns: CUSTOM_date [local], CUSTOM_updateTime [local], OSD.flyTime, OSD.flyTime [s], OSD.latitude, OSD.longitude, OSD.height [ft], OSD.heightMax [ft], OSD.vpsHeight [ft], OSD.altitude [ft], OSD.mileage [ft], OSD.HSpeed [MPH], and OSD.HSpeedRt. The data shows a flight starting at 8:16:58.15 PM and ending at 8:27:01.01 PM. The altitude increases from 93 feet to 95 feet, and the speed increases from 0 to 0.7 MPH. The battery level is shown as 0.223694 at the end of the flight.

CUSTOM_date [local]	CUSTOM_updateTime [local]	OSD.flyTime	OSD.flyTime [s]	OSD.latitude	OSD.longitude	OSD.height [ft]	OSD.heightMax [ft]	OSD.vpsHeight [ft]	OSD.altitude [ft]	OSD.mileage [ft]	OSD.HSpeed [MPH]	OSD.HSpeedRt
6/1/2023	8:16:58.15 PM	0m 0.0s	0.0	40.4564927295001	-74.4988311224086	0	0	0.3	93	0	0	0
6/1/2023	8:16:58.27 PM	0m 0.1s	0.1	40.45649282444029	-74.49883112360935	0	0	0.3	93	0	0	0
6/1/2023	8:16:58.37 PM	0m 0.2s	0.2	40.45649271963512	-74.49883117024413	0	0	0.3	93	0	0	0
6/1/2023	8:16:58.47 PM	0m 0.3s	0.3	40.45649269394374	-74.49883117533024	0	0	0.3	93	0	0	0
6/1/2023	8:16:58.57 PM	0m 0.4s	0.4	40.456492686677045	-74.49883118033336	0	0	0.3	93	0	0	0
6/1/2023	8:16:58.67 PM	0m 0.5s	0.5	40.45649266170485	-74.49883118211112	0	0	0.3	93	0	0	0
6/1/2023	8:16:58.77 PM	0m 0.6s	0.6	40.45649265933547	-74.49883119171223	0	0	0.3	93	0	0	0
6/1/2023	8:16:58.87 PM	0m 0.7s	0.7	40.45649263988207	-74.49883119013458	0	0	0.3	93	0	0	0
6/1/2023	8:16:58.98 PM	0m 0.8s	0.8	40.45649263650339	-74.49883118787994	0	0	0.3	93	0	0	0
6/1/2023	8:16:59.08 PM	0m 0.9s	0.9	40.45649261193472	-74.49883118512713	0	0	0.3	93	0	0	0
6/1/2023	8:16:59.18 PM	0m 1.0s	1.0	40.45649258295982	-74.49883119692093	0	0	0.3	93	0	0	0
6/1/2023	8:16:59.28 PM	0m 1.1s	1.1	40.4564923255296	-74.49883119787395	0	0	0.3	93	0	0	0
6/1/2023	8:16:59.38 PM	0m 1.2s	1.2	40.4564924738101	-74.49883119896725	0	0	0.3	93	0.1	0	0
6/1/2023	8:16:59.48 PM	0m 1.3s	1.3	40.45649241490602	-74.49883117322762	0	0	0.3	93	0.1	0	0
6/1/2023	8:16:59.59 PM	0m 1.4s	1.4	40.456492287670805	-74.498831039689	0	0	0.3	93	0.2	0	0
6/1/2023	8:16:59.69 PM	0m 1.5s	1.5	40.4564922542273	-74.49883100561925	0	0	0.3	93	0.2	0	0
6/1/2023	8:16:59.79 PM	0m 1.6s	1.6	40.45649223929625	-74.49883100161246	0	0	0.3	93	0.2	0	0
6/1/2023	8:16:59.89 PM	0m 1.7s	1.7	40.45649219229284	-74.49883103360773	0	0	0.3	93	0.2	0	0
6/1/2023	8:16:59.99 PM	0m 1.8s	1.8	40.456492100113145	-74.49883113296276	0	0	0.3	93	0.2	0.223694	0.223694
6/1/2023	8:17:00.09 PM	0m 1.9s	1.9	40.45649205351196	-74.49883129910198	0	0	0.3	93	0.3	0.316351	0.316351
6/1/2023	8:17:00.20 PM	0m 2.0s	2.0	40.4564919308429	-74.49883145494344	0	0	0.6	93	0.4	0.316351	0.316351
6/1/2023	8:17:00.30 PM	0m 2.1s	2.1	40.456491803050995	-74.49883163254573	0.3	0.3	0.6	93	0.4	0.316351	0.316351
6/1/2023	8:17:00.40 PM	0m 2.2s	2.2	40.456491675846486	-74.49883181725808	0.6	0.6	0.9	93	0.5	0.316351	0.316351
6/1/2023	8:17:00.50 PM	0m 2.3s	2.3	40.45649156450489	-74.4988320077871	0.9	0.9	1.3	94	0.6	0	0.316351
6/1/2023	8:17:00.60 PM	0m 2.4s	2.4	40.4564913892208	-74.4988321423209	1.3	1.3	1.6	94	0.6	0	0.316351
6/1/2023	8:17:00.70 PM	0m 2.5s	2.5	40.45649129084163	-74.49883221168336	1.6	1.6	1.9	94	0.7	0	0.316351
6/1/2023	8:17:00.80 PM	0m 2.6s	2.6	40.45649124119190	-74.4988323743693	1.9	1.9	2.6	95	0.7	0	0.316351
6/1/2023	8:17:00.91 PM	0m 2.7s	2.7	40.456491249197201	-74.4988323749144	2.2	2.2	2.9	95	0.7	0	0.316351
6/1/2023	8:17:01.01 PM	0m 2.8s	2.8	40.456491142481171	-74.49883237902529	2.6	2.6	3.2	95	0.7	0	0.316351

Figure.27 Aircraft log Analysis

- Deleted Artifacts:** - An autopsy can recover deleted data from any digital device using the forensic image file found in this investigation. This research study clearly shows that this SD card is already used in Android devices for data storage and transmission purposes. After using the same memory card in the drone to record images and videos, I was able to recover all erased files from the drone's SD card.

This section provides a description of the many kinds of data that can be recovered after it has been destroyed. There are a total of 25900 files that have been wiped from the SD card, as shown by the red cross in the screen shot, which indicates that data have been deleted during the autopsy.

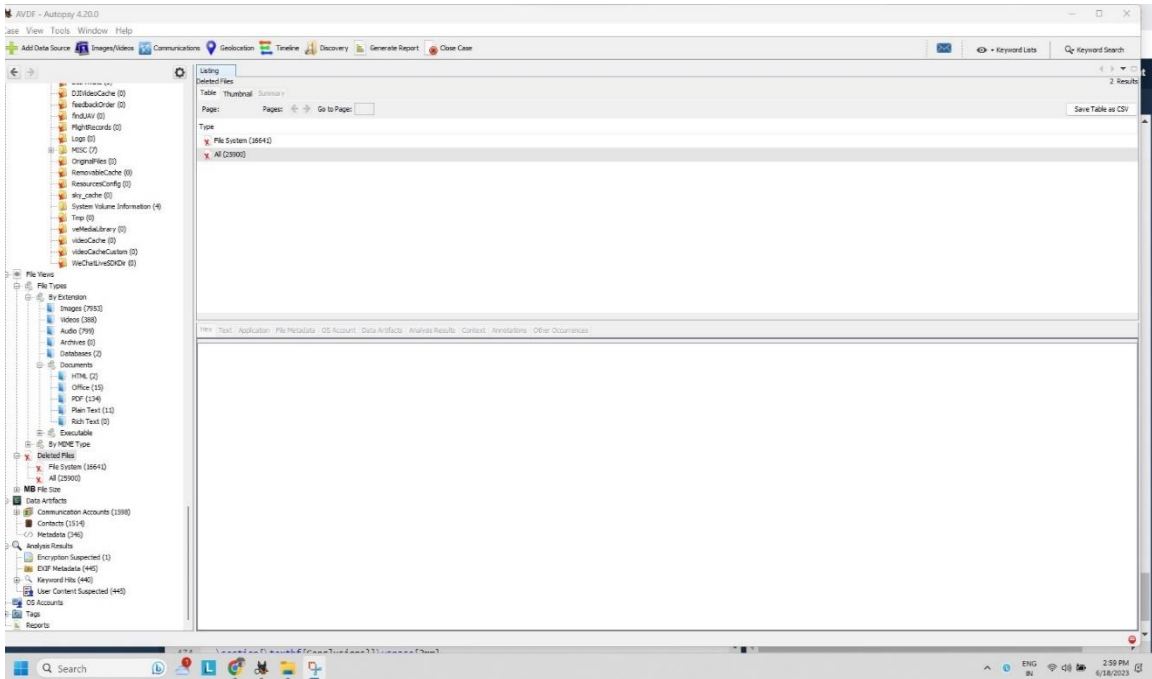


Figure.28 Deleted Data Information in Autopsy

Recoverable files that have been deleted, such as PDF and document files, can now be retrieved. During the autopsy, a conspicuous red cross is displayed on the screen, indicating the deliberate deletion of data. Within the application view, the data that has been deleted from the SD card is visible.

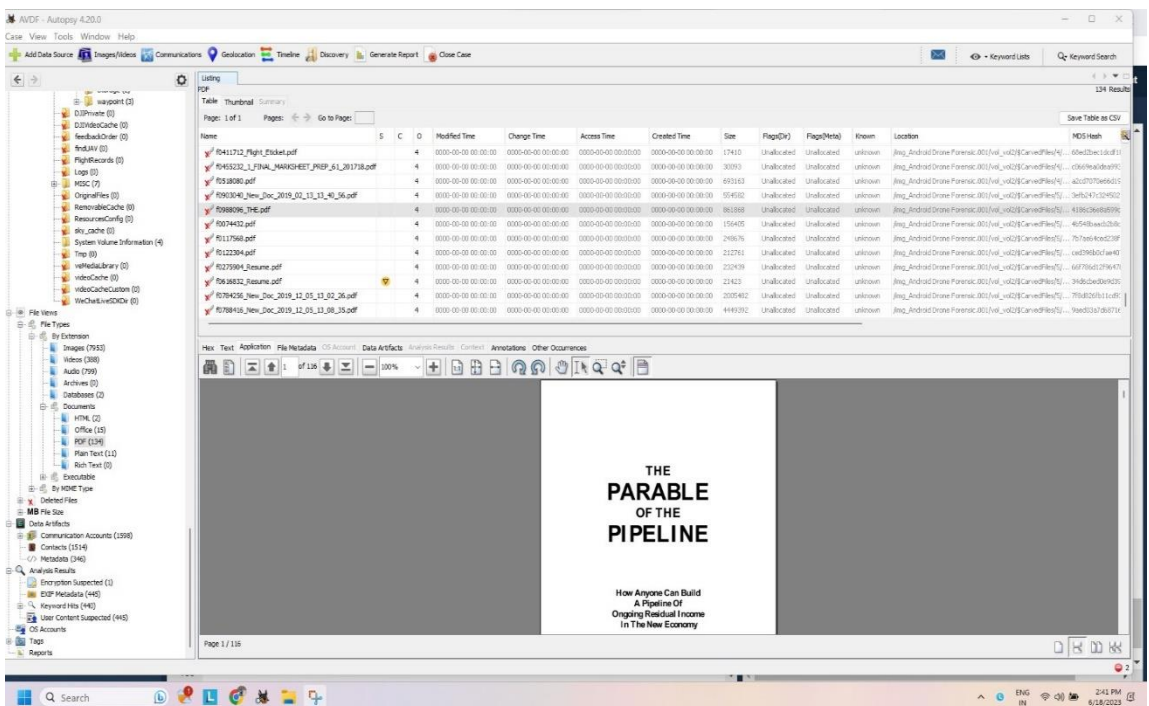


Figure.29 Deleted Documents Information in Autopsy

In the contact application view, we can see the true contact number as well as the user's name, which has already been removed from the SD card. This information is crucial in forensic investigations to solve crimes. I was successful in recovering all 1579 contact numbers and 17 email address information from the drone and all contact number and email address information is saved in .vcf file extension.

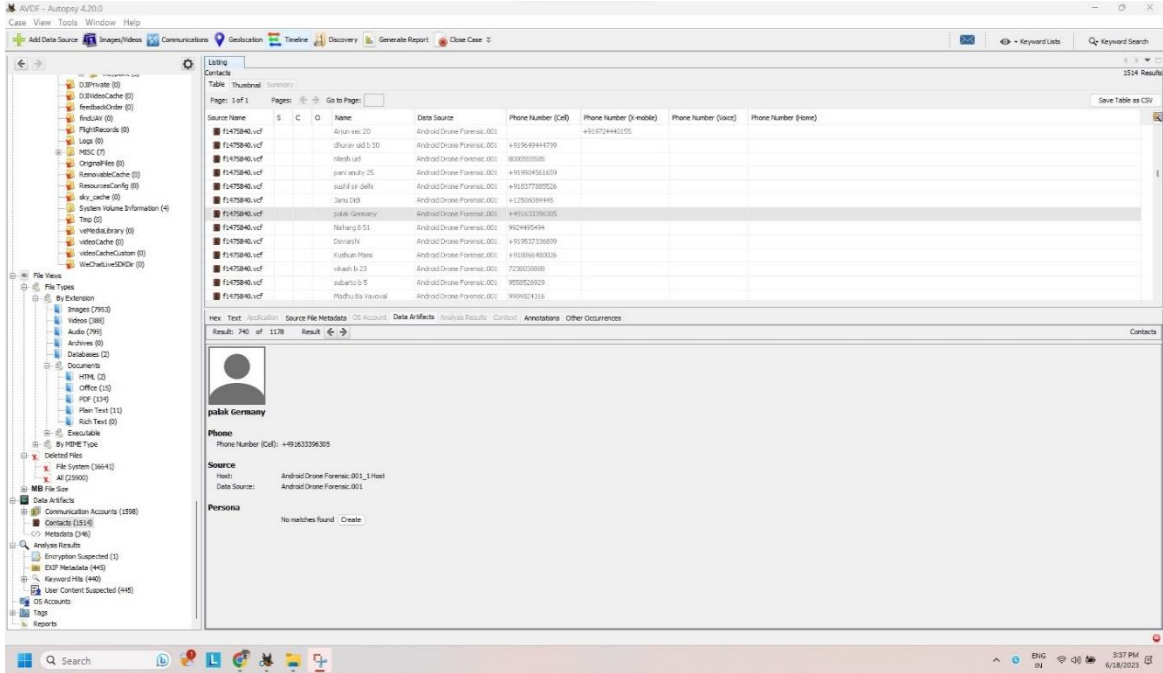


Figure.30 Deleted Contact Number Recover in Autopsy

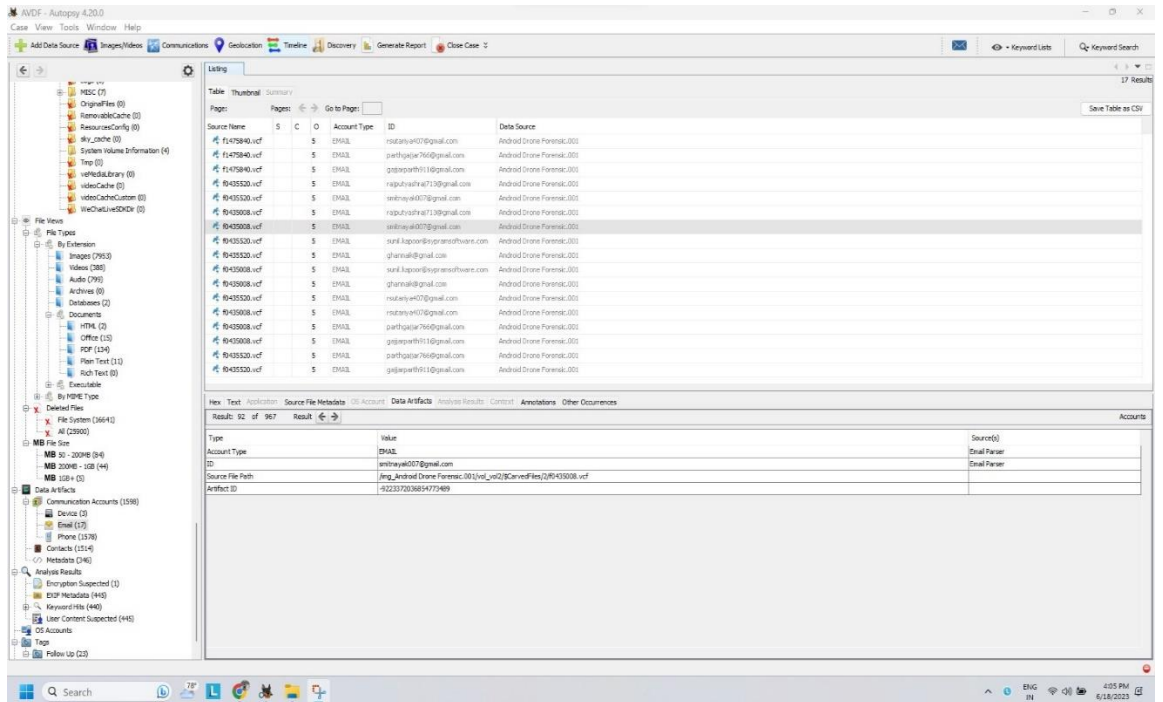


Figure.31 Deleted Email Information Recover in Autopsy

In this research study, I discovered the most essential leading information from the data. I discovered several flight records files that have previously been wiped from the memory card in my Android phone, proving indirectly that the drone has been used many times to gather certain information. and I was able to successfully restore all deleted drone flight log files from the smartphone. The image below displays the deleted flight log files, which are marked with a red cross.

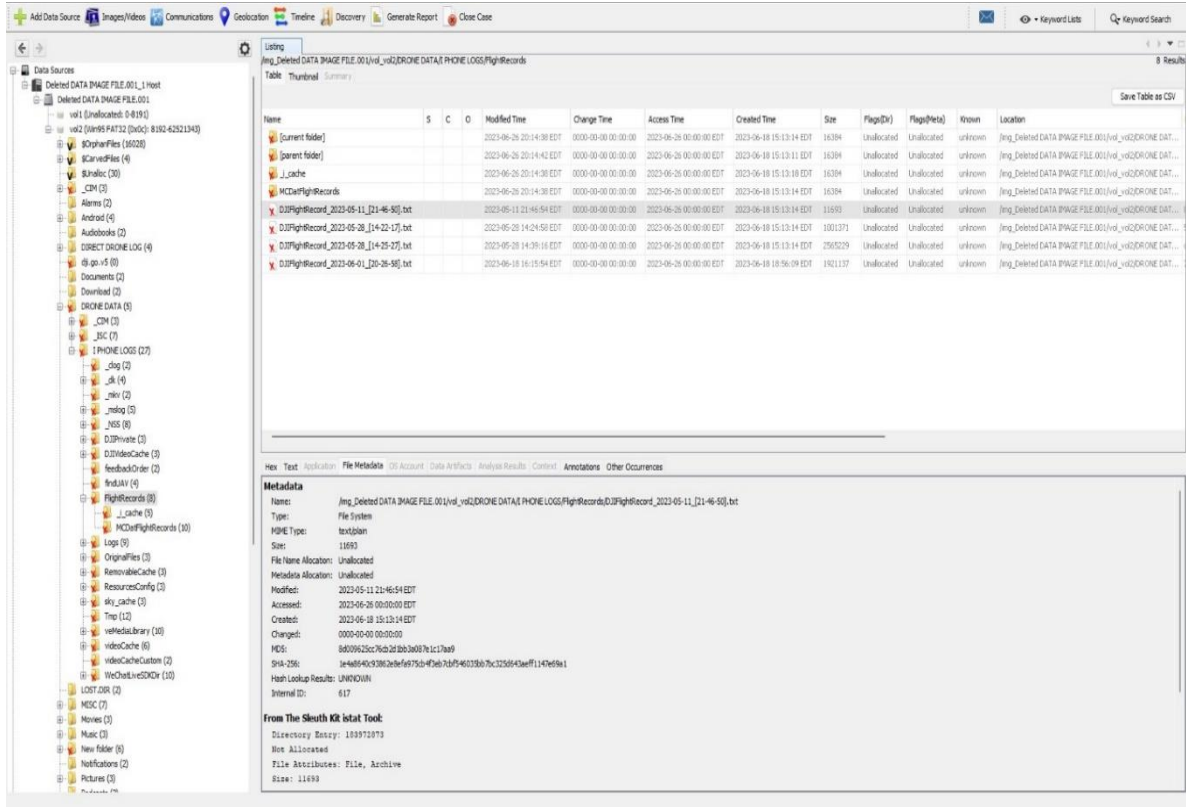


Figure.32 Deleted Drone Flight Log Files Recovery

Following the extraction of the drone flight log files that had been removed, I utilized the air data application to extract further information from the drone log files that had been destroyed. As a result, I found the following information regarding drone flights.

The image that is displayed above illustrates the flight parameters of the drone. These parameters include the following: flight duration of **14 minutes and 43 seconds**, time, and date of **June 5th, 2023, 7:56 PM**, minimum flight height of **399 feet**, maximum flight height of **506.6 feet**, battery percentage information during takeoff of **100%** and landing time of **45%**, weather information and wind speed of **20.67 miles** per hour, total distance traveled of **3819 feet**, including information about photos that were captured.

In this observation, I discovered that the drone is flying in a different location.

Figure.33 Deleted Drone Flight Log Analysis with Different Location in Air-data

In this research, I uncovered deleted photos and video material captured by a drone in an autopsy, as well as information on the date and time 2023-06-05,20:05PM for that specific image and video taken from the drone.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location	MD5 Hash
JI_0064.JPG				2023-06-05 19:59:34 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 19:59:34 EDT	4125971	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	79a6d75d7aeb286f92882
JI_0066.JPG				2023-06-05 20:02:16 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:02:16 EDT	4046396	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	c614d05d8d8f8d907012b
JI_0068.JPG				2023-06-05 20:04:36 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:04:36 EDT	4461719	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	4664836d26640b3cc6a83
JI_0070.JPG				2023-06-05 20:04:36 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:04:36 EDT	4158787	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	e1c15a30a850307d2b0f99
JI_0072.JPG				2023-06-05 20:04:38 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:04:38 EDT	4299796	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	96931b6c72432f265e40b1
JI_0074.JPG				2023-06-05 20:04:40 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:04:40 EDT	3989901	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	20f448f5c8f076a0df7019
JI_0076.JPG				2023-06-05 20:04:42 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:04:42 EDT	3866785	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	7f04c499a3084f413e0900
JI_0078.JPG				2023-06-05 20:04:44 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:04:44 EDT	4935520	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	5a160a79744a721b8325
JI_0080.JPG				2023-06-05 20:04:48 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:04:48 EDT	4278200	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	6f1a00401a665636773b28
JI_0082.JPG				2023-06-05 20:04:50 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:04:50 EDT	4463019	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	22b2e4e371acc6b311d2f
JI_0084.JPG				2023-06-05 20:05:42 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:05:42 EDT	4952324	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	d38707a9c35a93f424b48e
JI_0086.JPG				2023-06-05 20:05:44 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:05:44 EDT	4952115	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	d54410a65449d8f0c0e08c
JI_0088.JPG				2023-06-05 20:05:46 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:05:46 EDT	4248478	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	9f0d77308acc39830f45f
JI_0090.JPG				2023-06-05 20:05:48 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:05:48 EDT	4241727	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	c1d2a628b011ea53d0f9541
JI_0092.JPG				2023-06-05 20:05:50 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:05:50 EDT	4075207	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	6d0338c2a90c4e3d80311
JI_0094.JPG				2023-06-05 20:05:52 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:05:52 EDT	4770880	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	4112ab33c1c1574982493a
JI_0096.JPG				2023-06-05 20:05:54 EDT	0000-00-00 00:00:00	2023-06-26 00:00:00 EDT	2023-06-05 20:05:54 EDT	4767598	Unallocated	Unallocated	unknown	Jimg_Deleted DATA IMAGE FILE.001\vol_v02\CSM_00ME...	089435a47f68b02b2c247

Figure.34 Deleted Drone Photo Video Recovery in Autopsy

5.4 Future Challenges in Drone forensic.

Now, every drone that is available on the market comes with its own storage system, which is an SD Card. However, as technology continues to improve and drones begin to use cloud storage systems for the purpose of storing data as forensic investigators, the possibility of data recovery becomes more challenging. Two-way encryption and the most cutting-edge algorithms are utilized by cloud storage systems to ensure the confidentiality of data. An adversary could simply assault and destroy all the information stored on the cloud storage server, including the data pertaining to drone logs. In this scenario, if the drone is equipped with a highly powerful and entirely remote controller that is also equipped with a cloud storage system, then something has occurred, and we do not have any tracing lead information to locate the operation of the drone.

6. CONCLUSIONS

The rising availability of drones, as well as technological improvements, have increased the possibility of their unlawful usage. The capacity to track down and present proof of illegal drone use is critical when a case gets to court. I was able to extract data from the drone forensic picture file that was returned after the drone was discovered at the crime scene by doing data forensics on it. To perform a forensic investigation, I used a free tool called autopsy and air data, DJI assistant, and FTK imager. This provided us with a better opportunity to analyze the drone data, and with the help of the tools, I was able to effectively recover all information including many locations of that drone flight fly, even erased data, stored on the drone's SD card. All the data is in various formats. We can see contact number information together with a name. One thing I noticed is that the DJI SE 2 Mini drone does not have a large battery capacity, thus it cannot fly for longer than 20 minutes. However, the DJI drone includes a powerful fully remote receiver that allows it to fly more than 1000 feet in the air. As an option, it is the most dangerous and illegal, and it may easily be run by long distances for spying or any terrorist purpose.

Future research should prioritize doing thorough security assessments of many widely used consumer drone models and developing and executing efficient countermeasures to address the identified vulnerabilities. An investigation on the influence of developing technologies, such as artificial intelligence and block chain, on the security of drones. This research could be used to build and test defense mechanisms that are both effective and precise against cyber problems in data recovery from drones. Based on the findings of this research, it is imperative to promptly enforce enhanced safety measures in consumer drones, such as the DJI Mini SE 2. The identified vulnerabilities pose significant risks to the privacy and security of users, as well as the integrity of their data. Because the DJI drone mobile application does not encrypt any data, hackers can install Rat on an Android device and get control of the drone controller. Collaboration between drone manufacturers, regulatory agencies, and cybersecurity specialists is vital to address these weaknesses and establish robust security protocols, thereby minimizing the threat of cyberattacks in the dynamic realm of drones.

REFERENCES

- [1] Carlier, M, "Commercial drone market revenue worldwide projection. statista," 2023, 2 May.
- [2] E. Mantas and C. Patsakis, "Who watches the new watchmen? The challenges for drone digital forensics investigations," *Array*, vol. 14, p.100135, 2022.
- [3] G. Maeakafa, "Establishing effective and economical surveillance for traffic," 12 2016.
- [4] L. Hern´andez-Hern´andez, A. Tsourdos, H.-S. Shin, and A. Waldock, "Multi-objective uav routing," 2014 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 534–542, 2014.
- [5] E. Mantas and C. Patsakis, "Gryphon: Drone forensics in dataflash and telemetry logs," in *Advances in Information and Computer Security*, N. Attrapadung and T. Yagi, Eds. Cham: Springer International Publishing, 2019, pp. 377–390.
- [6] D.-Y. Kao, M.-C. Chen, W.-Y. Wu, J.-S. Lin, C.-H. Chen, and F. Tsai, "Drone forensic investigation: Dji spark drone as a case study," *Procedia Computer Science*, vol. 159, pp. 1890–1899, 2019, knowledge-Based and Intelligent Information Engineering Systems: Proceedings of the 23rd International Conference KES2019.
- [7] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of things (iot): A literature review," *Journal of Computer and Communications*, vol. 3, pp. 164–173, 04 2015.
- [8] Z. Baig, M. A. Khan, N. Mohammad, and G. B. Brahim, "Drone forensics and machine learning: Sustaining the investigation process," *Sustainability*, vol. 14, no. 8, 2022.
- [9] 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, 2021.
- [10] U. Jain, M. Rogers, and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," in *2017 IEEE Sensors Applications Symposium (SAS)*, 2017, pp. 1–6.
- [11] M. Yousef, F. Iqbal, and M. Hussain, "Drone forensics: A detailed analysis of emerging dji models," in *2020 11th International Conference on Information and Communication Systems (ICICS)*, 2020, pp. 066–071.
- [12] S. C. Nayak, V. Tiwari, and B. K. Samanthula, "Review of ransomware attacks and a data recovery framework using autopsy digital forensics platform," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 2023, pp. 0605–0611.
- [13] Wikipedia contributors, "Forensic toolkit — Wikipedia, the free encyclopedia," 2023, [Online; accessed 3-June-2023].
- [14] R. Hossain, "A short review of the drone technology," vol. 7, p. 16, 08 2022.

- [15] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs) practical aspects, applications, open challenges, security issues, and future trends.
- [16] M, "Github - Morsmalleo/AhMyth: Cross-Platform Android Remote Administration Tool | Official maintained repository for the AhMyth R.A.T Project.
- [17] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. Alsharif, and M. Khan, "Unmanned aerial vehicles (uavs): Practical aspects, applications, open challenges, security issues, and future trends," *Intelligent Service Robotics*, 01 2023.
- [18] Drone Hacking Tool Analysis: Dronesplit - DroneSec," <https://dronesec.com/blog/drone-hacking-tool-analysis-dronesplit>.
- [19] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. Lauf, L. Watkins, W. Robinson, and W. Alexis, "Securing commercial wifi-based uavs from common security attacks," 11 2016.
- [20] S. C. Nayak, V. Tiwari, and B. K. Samanthula, "Review of ransomware attacks and a data recovery framework using autopsy digital forensics platform," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), 2023*, pp. 605–611.
- [21] What is RAT cybercrime? - The Menace of RAT Malware, <https://cyberpedia.reasonlabs.com/EN/rat>
- [22] McAfee, "What is a Remote Administration Tool (RAT)?" 2 2024. [Online].
- [23] S. Awasthi, P. K. Srivastava, N. Kumar, R. P. Ojha, and A. K. Yadav, "A Study of the Dissemination of Malware and the Enhancement of the Lifespan of Rechargeable Wireless Sensor Networks: An Epidemiological Approach.
- [24] International crackdown on RAT spyware, which takes total control of victims' PCs Europol.
- [25] Remote Access Trojans (RATs): the silent invaders of cybersecurity." [Online].
- [26] K. Andre and K. Andre, "Remote Access Trojans Explained plus 17 Best RAT Software, Scanners, amp; Detection Tools.
- [27] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, 04 2019.
- [28] M. Corporation, "Backdoor:AndroidOS/Ahmyth.A!MTB threat description- Microsoft Security Intelligence," 8 2020. [Online].
- [29] M. Shihab, "Android application to monitor and protect from remote access trojan," 09 2018.
- [30] S. F. Everyone, "2021 Mobile Malware Statistics <https://securityforeveryone.com/blog/2021-mobile-malware-statistics>.
- [31] Transparent Tribe's new Android spyware distributed under the guise of popular apps," 5 2021. [Online].

- [32] V. Hassija, V. Chamola, A. Agrawal, and M. Guizani, "Fast, Reliable, and secure drone Communication: comprehensive survey," ResearchGate, 5 2021. [Online].
- [33] L. Varghese, R. J. Tomy, J. Thomas, and N. Jacob, "Securing Android Phones against Potential Thefts: AhMyth Android RAT," 2020. [Online].
- [34] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, "Cyber4drone: A systematic review of cyber security and forensics in next-generation drones," *Drones*, vol. 7, no. 7, 2023.
- [35] Galaxy M20 | Samsung Jordan," 9 2020. [Online].
- [36] S. Nayak, B. K. Samanthula, and V. Tiwari, "Investigating drone data recovery beyond the obvious using digital forensics," in *2023 IEEE 14th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, 10 2023, pp. 0254–0260.
- [37] G. Baran, "Android Rat - Hack Targeted Android Phone," 11 2023. [Online].
- [38] D. Aprilliansyah, I. Riadi, and S. Sunardi, "Analysis of remote access trojan attack using android debug bridge," *IJID (International Journal on Informatics for Development)*, vol. 10, pp. 102–111, 02 2022.
- [39] R. Satrio Hadikusuma, L. Lukas, and E. Rizaludin, "Methods of stealing personal data on android using a remote administration tool with social engineering techniques," *Ultimatics : Jurnal Teknik Informatika*, pp. 44–49, 06 2023.
- [40] DJI Flight Log Viewer | Phantom Help." [Online].