Forensic Analysis of the DJI Phantom 4 Pro V2.0: Techniques, Challenges, and Applications

Ratnesh Dwivedi, Pallavi Khatri, Animesh Kumar Agrawal, Diya Khatri

Email id1, emaliid 2, emailed 3, emailed 4

Affiliation1

Affiliation 2

Affiliation 3

# ABSTRACT

Drones are being used extensively for commercial purposes and in criminal activities too, world over. In order to gather evidence from the captured drones, it is imperative that sources of evidence are explored to gather evidence against the perpetuator of crime. The DJI Phantom 4 Pro V2.0 is a widely used drone with advanced capabilities, making it a common subject in forensic investigations. This paper explores the methodologies for conducting forensic analysis on this specific drone model. It covers data acquisition techniques, analysis of various data types, challenges encountered in the forensic process, and the applications of these forensic methods in real-world scenarios. The study aims to contribute to the understanding and development of drone forensics by providing a comprehensive analysis of the DJI Phantom 4 Pro V2.0.

Keywords: Drone Forensics. DJI Phantom 4, Digital forensics, UAV Forensics

# INTRODUCTION

Unmanned aerial vehicles (UAV’s), commonly known as drones, are operated and controlled remotely and are used for defense and rescue missions. Drones are mainly used for defense purposes (for example, they were widely used in the war between Ukraine and Russia), but in recent years their use for civilian purposes has increased significantly drones are used for tasks such as patrolling and policing, search and rescue, agricultural technology and filming, as well as deterring and identifying poachers due to the dominance of digital lifestyle. The popularity and affordability of drones has also increased their use in illegal activities. Investigations rely heavily on drone recovered from the crime scene and the devices attached to it. Evidence can be collected from drone and its ground controller, including drone identification number, location of previous flight, camera footage, logs and software used. As the number of drones in operation continues to increase, security, privacy and security concerns are expected to increase. The drone relies on a network of sensors and actuators to establish communication with the GCS (Ground Control System) through wireless links. A possible chain of events revealed that a combination of cyberattacks had been launched, in which all communication with the initial drone was cut off as jammed control signals as well satellite and ground. Drones represent the flying objects of the Internet of Things, combining hardware with control software. Drones Communicate with the smart device over a WIFI channel for short distances with frequency of 2.4 GHz or 5 GHz [1][2][3]. They are programmed and equipped well with Sensors, cameras for data collection and are operated by a GPS operators to perform any desired operation. This makes it more important to develop strong security protocols to prevent intrusion and misuse of drones. Drones are widely used nowadays by multiple industries for various purposes like law enforcement agencies use it for safety and security, rescue missions etc. Agriculture industry use the same drone for seed and fertilizer dispensing, Health care industry use it for drug delivery and Food industry is using it for food delivery. Wide usage of drones in industries and their accessibility in to the remote and inaccessible regions due to their size and ease of operability have posed a challenge to the security agencies to the events where drones can be programmed to exploit any industry, country or individual and performing criminal activities. It is challenging to efficiently monitor and control drones because of their covert and remote control features. In order to reduce the possibility of drone operators being abused in criminal activity, digital forensic research has become a significant field of interest in response to these concerns, particularly in the late 2010s. Challenges are further added due to the everchanging coding of flight and lack of research into the modern remote controls that are now integrated into the instrument panel. Furthermore, the ever-changing drone market, which is marked by frequent product launches and developing remote control technology, necessitates large time, effort and resource commitments to digital forensic research in order to stay updated with developments and successfully handle emerging challenges.

Drones can function independently or with remote control due to a variety of technologies, such as computer vision, artificial intelligence, and obstacle avoidance. The identification of drone operators and the determination of whether or not drones are engaged in illegal activities depend on precise forensic analysis of drone data. Extracting information about the location of drone and related devices is crucial for conducting in-depth forensic investigation and apprehending malevolent attackers.

Drone forensics a subset of digital forensics presents unique difficulties due to the intricate relationships between software containers and hardware artifacts. Because of their affordability adaptability and ability to collect and analyze data effectively in hazardous or remote environments drones are immensely helpful in a wide range of fields. As demonstrated by instances of drones colliding with manned aircraft operating in restricted airspace and interfering with vital infrastructure the extensive use of drones however presents safety and security issues.

Stakeholders must work together as the drone industry expands to resolve these problems and ensure the moral and responsible use of drones. In order to create comprehensive strategies that support the responsible safe and secure introduction of drones into society governments business leaders and researchers must collaborate. According to cyber security standards drones security feature—which ensures confidentiality integrity availability and confidentiality—is essential. However, the widespread use of drones has caused challenges for many countries such as issues with security policy and regulation software development and a lack of technological monitoring and detection. A significant number of drone accidents have happened at vital locations in recent years such as airports, prisons and borders. Drone investigations are difficult due to their proprietary nature and the large variety of drones in the market. A unified drone investigation platform that can examine flight logs from well-known drone manufacturers including DJI, Yuneec, and 3DR has been established in order to address these issues. The platform aims to visualize drone flight information, including a 3D representation of the flight path using Google Maps, and evaluate the results according to FAA regulations [4][5][6][7].

The expansion of UAVs has led to challenges, countering airspace clog and security concerns, with an uptick in collision occurrences. Conventional strategies battle to oversee this convergence due to the interesting activity designs and innovation of UAV. The scattered nature of information in UAV systems, including different gadgets like switches, and sensor hubs, requires cautious arranging for viable information extraction and legal examination. Moreover, known as unmanned airborne vehicles, drones are progressively well known due to their availability and reasonableness, driving to a surge in worldwide commercial markets and drone-related wrongdoings. The rise in criminal exercises including rambles underscores the basic requirement for legal investigation to accumulate data from onboard sensors, hardware, and cameras to distinguish suspects and avoid encouraging wrongdoings. Be that as it may, translating flight information and tending to the multi-platform nature of rambles poses critical challenges in legal investigation. Be that as it may, the complexity and assortment of UAVs posture challenges, with existing DRF models missing an organized and bound together system for overseeing and sharing errands and exercises [8][9][10].

The advancement of such a system may essentially improve the productivity and viability of measurable examinations. The use of unmanned aerial vehicles is increasingly popular, especially among hobbyists, photographers, and journalists, with the number of licensed pilots. However, this accessibility has posed challenges in the field of digital forensics, leading INTERPOL to collaborate with various stakeholders to develop a drone incident response framework to resolve legal challenges. Classification of artifacts recovered from drones is critical to improving the investigation and response to drone incidents. The Computational Reference Data Set provides access to drone imagery and data obtained from various drone models. Additionally, cyber threats pose a significant challenge to the reliability of digital evidence in the drone ecosystem. The drone industry has seen notable growth, with market predictions estimating it will reach nearly $60 billion by 2025, driven by an increase in drone shipments, consumer ridership and the industry's public and private demand and is expected to reach approximately $100 billion in the near future. However, with the growth of the industry, illegal activities involving the drones have also increased, with 367 incidents reported in the United States by the Federal Aviation Administration between October and December 2020. The FAA works closely with law enforcement to investigate and respond to these incidents [9].

# LITERATURE SURVEY

Drone forensics is an expanding field that investigates Unmanned Aerial Vehicles (UAVs) for purposes such as law enforcement, security, and privacy. Researchers focus on extracting and analyzing data from drone components like flight controllers, memory chips, and onboard cameras, as well as reconstructing flight paths and identifying UAV operators. Using concepts from computer science, digital forensics and engineering, this multidisciplinary field focuses on creating tools specifically designed to address the particular difficulties posed by drones. By making it easier to extract, visualize and interpret data these tools aid analysts in reconstructing timelines and looking into incidents. Challenges like managing encrypted data, preventing GPS spoofing and differentiating between malicious and legitimate activity are revealed by case studies and real-world applications. Additionally interdisciplinary cooperation between government, businesses and academia guarantees a thorough approach to resolving ethical and legal issues such as privacy, the admissibility of evidence and regulatory compliance. Drone forensics raises a number of ethical questions in criminal investigations but the main ones are privacy, responsibility and misuse potential. Establishing moral guidelines that control drone use is essential as they become more and more integrated into law enforcement in order to preserve civil liberties and maintain public safety. Drones have many advantages when used in forensic investigations but there are also moral issues that need to be resolved to avoid rights abuses and guarantee responsible use. It is essential to strike a balance between these factors in order to preserve public confidence in police tactics. The use of drones for surveillance in public areas like demonstrations or meetings can violate people’s right to privacy. Drone data collection raises concerns regarding data security and the possibility of personal data being misused [11]. Since there are no explicit rules on how evidence should be gathered and processed the absence of standardized procedures for drone forensics makes accountability more difficult [8]. For law enforcement agencies to function openly and preserve public confidence a drone-specific code of conduct must be established [12]. There are ethical concerns about the use of drones in law enforcement because they can be weaponized or misused [13]. Because drones can be used as both forensic tools and possible criminal tools they must be carefully regulated to avoid misuse [14].

In order to reconstruct flight path, the UAV needs to be located and the identity of the operator needs to be established so that data can be extracted from the drone as well as the drone controller. GPS forensics—a crucial subset of drone forensics—focuses on analyzing GPS data. Geospatial analysis includes GPS data extraction and correlation with timestamps and other data sources. Researchers are working to create tools that improve these analysis, precision and dependability by addressing flaws like GPS jamming and spoofing. Difficulties in these situations include identifying malicious activity from legitimate activity and signal degradation in urban settings. A major part is also played by communication forensics which involves intercepting and analyzing cellular Wi-Fi and radio frequency signals sent back and forth between UAVs and their control systems. By using tools created in this field analysts can decrypt communications and piece together events enabling them to spot dangers or bad actors.

These developments which draw on knowledge from geospatial science cybersecurity and telecommunications emphasize the value of interdisciplinary cooperation. Emerging fields such as physical forensics and malware analysis enhance the larger scope of drone investigations. Malware forensics investigates threats against UAV systems emphasizing compromised systems malware distribution methods and mitigation techniques. The intricacy of this field is highlighted by real-world examples such as researching payloads aimed at UAV flight controllers. Similar to this physical forensics looks into how hardware parts interact with digital evidence allowing analysts to link physical damage to camera images or flight data. Drone-captured visual data is analyzed by image and video forensics to verify content integrity identify objects and reconstruct events. Modern tools and algorithms make it easier to identify objects and reconstruct scenes increasing the validity of visual evidence in court. Improving the dependability security and accountability of drone technology across industries is the goal of these multidisciplinary initiatives which span disciplines like materials science engineering and digital forensics.

Because drone technology is developing so quickly the data involved is complex and there are no established methods analyzing drone crash data for forensic purposes is fraught with difficulties. These difficulties impede efficient research and call for a thorough comprehension of the special traits of drones and their operating environments. The speed at which drone technology is developing frequently surpasses forensic standards updates making it more difficult to evaluate the accuracy and dependability of new tools [15]. Data analysis and evidence gathering become more complex when cutting-edge technologies like machine learning and image processing are integrated [16]. Assuring data integrity and repeatability during forensic examinations is made extremely difficult by the large amount of software data produced by drones [2]. The justification of results in forensic investigations is complicated by problems with the traceability of both static and live digital evidence [2]. Standardized forensic processes specific to drone technology are desperately needed since current approaches frequently fall short in addressing the particular difficulties presented by UAVs [8]. Inconsistencies in the collection and processing of evidence are caused by the absence of a unified Drone Digital Forensics Investigation Framework [8]. Notwithstanding these obstacles research into more efficient techniques and frameworks is continuing and the field of drone forensics is changing. However forensic analysts continue to face many challenges due to the variety of operational contexts and the quick advancements in technology.

The DJI Phantom 4 Pro V2. 0 is a well-known drone that is renowned for its innovative features, excellent camera and dependable operation. The intricacy of data extraction and the dynamic nature of drone technology present forensic analysts with a number of difficulties when working with DJI Phantom drone data. These issues can be resolved with better techniques and drone forensics-specific tools. From identifying evidence to reporting these difficulties affect different phases of forensic investigations. The main issues noted in the literature are outlined in the sections that follow.

Data Types: Evidence extraction is made more difficult by the variety of data types that drones such as the DJI Phantom store such as flight logs photographs and personally identifiable information [17]. Internal vs. External Data: Analysts have to retrieve information from internal chip memory as well as external TF cards which can be challenging due to proprietary file structures and encryption [18]. Different File Types: A variety of file types are used by different DJI models (e. g. G. DAT TXT) making specialized parsers necessary for efficient data recovery [18] causes issues with data extraction.

Enhanced Security: Newer models have enhanced security features that make it harder for investigators to access essential data and impede forensic analysis [19]. Quick Technical Development: Analysts find it challenging to stay up to date with the rapid advancements in drone technology which frequently surpass the capabilities of forensic tools [20].

Data Integrity and Traceability: Its critical to maintain the integrity of the data gathered for forensic investigations because any changes could jeopardize the reliability of the evidence [2] presents both an operational and technical challenge.

Inadequate Guidelines: Since UAVs cannot be fully covered by current forensic guidelines such as those from ACPO and NIST customized protocols must be developed [21].

Lack of Standardization: Inconsistencies in the gathering and analysis of evidence result from the lack of standardized protocols for drone forensics [8].

Applications of Machine Learning: Incorporating machine learning into drone operations poses difficulties for intrusion detection and attack classification making forensic investigations more difficult [16].

**Proposed Solutions**

* **Standardized Methodologies**: Establishing standardized protocols for drone forensics can enhance the reliability of evidence collection and analysis [16].
* **Collaboration and Training**: Increased collaboration among forensic experts and ongoing training can help analysts adapt to new technologies and methodologies [1].

While these challenges are significant, the field of drone forensics is evolving, and ongoing research is likely to yield more effective tools and techniques to address these issues. However, the potential for anti-forensic techniques and the need for regulatory frameworks remain critical concerns that could hinder progress in this area [2][1].

This section discusses some key features and specifications of DJI Phantom Pro V2.0:

**Key Features:**

1. **Camera Quality:**
   * 1-inch 20MP CMOS sensor
   * Mechanical shutter to reduce rolling shutter distortion
   * 4K/60fps video recording
   * H.264 and H.265 video compression
2. **Flight Performance:**
   * Maximum flight time of approximately 30 minutes
   * Maximum control range of up to 7 kilometers (4.3 miles) with the DJI OcuSync 2.0 transmission system
   * Top speed of 72 kph (45 mph) in Sport Mode
3. **Obstacle Sensing:**
   * 5-direction obstacle sensing
   * 4-direction obstacle avoidance
4. **Intelligent Flight Modes:**
   * ActiveTrack
   * TapFly
   * Draw Mode
   * Gesture Mode
   * Waypoints
   * Point of Interest (POI)
   * Return to Home (RTH)
5. **Remote Controller:**
   * Built-in display (5.5-inch, 1080p)
   * Integrated OcuSync 2.0 for low-latency HD video transmission
6. **Build Quality:**
   * Sturdy, lightweight design
   * Foldable propellers for easy transport
   * **Advantages:**

* High-quality camera capable of capturing stunning aerial photos and videos.
* Long flight time and extended control range.
* Advanced obstacle sensing and avoidance for safer flights.
* Various intelligent flight modes for creative shooting options.
* Reliable and robust performance in different environments.
* **Disadvantages**
* Higher price point compared to some other consumer drones.
* Larger and less portable than some compact drone models.
* Requires some familiarity with drone operation to utilize all features effectively.
* **Use Cases**
* Professional aerial photography and videography
* Surveying and mapping
* Search and rescue operations
* Recreational flying for enthusiasts who demand high performance and quality

Using their sophisticated data collection and analysis capabilities forensic analysts take advantage of the features of DJI Phantom drones to obtain important evidence for investigations. For the purpose of reconstructing crime scenes and identifying suspects these drones offer real-time video feeds, flight logs and high-resolution imagery. The use of these features in forensic investigations is explained in detail in the sections that follow.

**Data Collection Capabilities**

* **High-Resolution Imaging**DJI drones help document crime scenes from multiple perspectives by taking detailed aerial photos [22].
* **Flight Logs**: Drones such as the DJI Phantom are capable of storing flight data such as GPS coordinates and timestamps which can be used to track the drones operator and usage[20] [23] .

**Real-Time Evidence Detection**

* **Live Streaming**: By transmitting live video forensic teams can keep an eye on ongoing events and collect evidence instantly improving situational awareness [23].
* **Computer Vision Techniques**: The incorporation of computer vision techniques can enhance the precision of evidence detection enabling the recognition of objects and individuals in recorded video [22].

**Data extraction that is non-invasive**

* **Forensic Analysis Tools**: DJI drones can be examined non-invasively to safeguard data integrity and extract useful digital artifacts [24].

In the continuing discussion about drone technology in law enforcement privacy concerns and the possibility of abuse in surveillance operations must be addressed even though DJI drones provide substantial benefits in forensic investigations.

# METHODOLOGY

While some drones store data in plain text, DJI drones store information in a format which is proprietary and encrypted. Hence, if log files are read directly they do not give any meaningful information. The logs need to be decrypted and then analysed. The methodology followed to analyse the logs is as brought out. Getting a physical drone for research and analysis was a challenge. To overcome this challenge Computer Forensic Reference DataSet Portal (CFReDS) portal of NIST was referred to and drone image of DJI drone was downloaded [25][26]. The downloaded data set contained both the internal and external SD card data on which analysis was done.

Step 1. Check if the log files are in plain text or encrypted.

Step 2. If encrypted, decrypt the same using tools like Flight Reader or Magnet Axiom to obtain the log files.

Step 3. Convert the log files in .csv format for ease of analysis

Step 4. Select and segregate the flight path reconstruction related parameters.

Step 5. Plot the path using an open source tool on a 3D map.

The path of the drone images is brought out in Figure 1. It contains various folders under the type of drone being analysed which includes the mobile app data, external SD card and internal memory data.

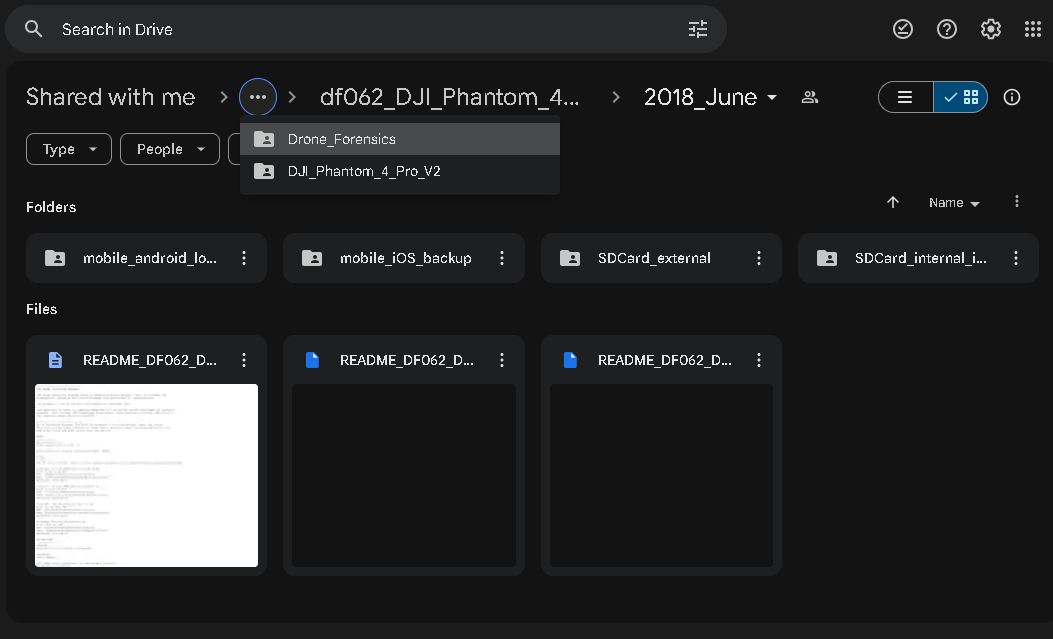


Figure 1. Drone image path

The SD Card\_internal\_intact was analysed in Autopsy which is an open source tool to carry out forensic analysis of different digital devices. Various files of flight logs namely FLY000.DAT, FLY001.DAT, FLY002.DAT, FLY003.DAT, FLY004.DAT, FLY005.DAT, FLY006.DAT, FLY007.DAT, FLY008.DAT, FLY009.DAT, FLY010.DAT were found. These files are created automatically by the drone as it flies and logs keep getting generated.

Encrypted files SYS.DJI, PARM, USER files were extracted in a different folder for analysis.

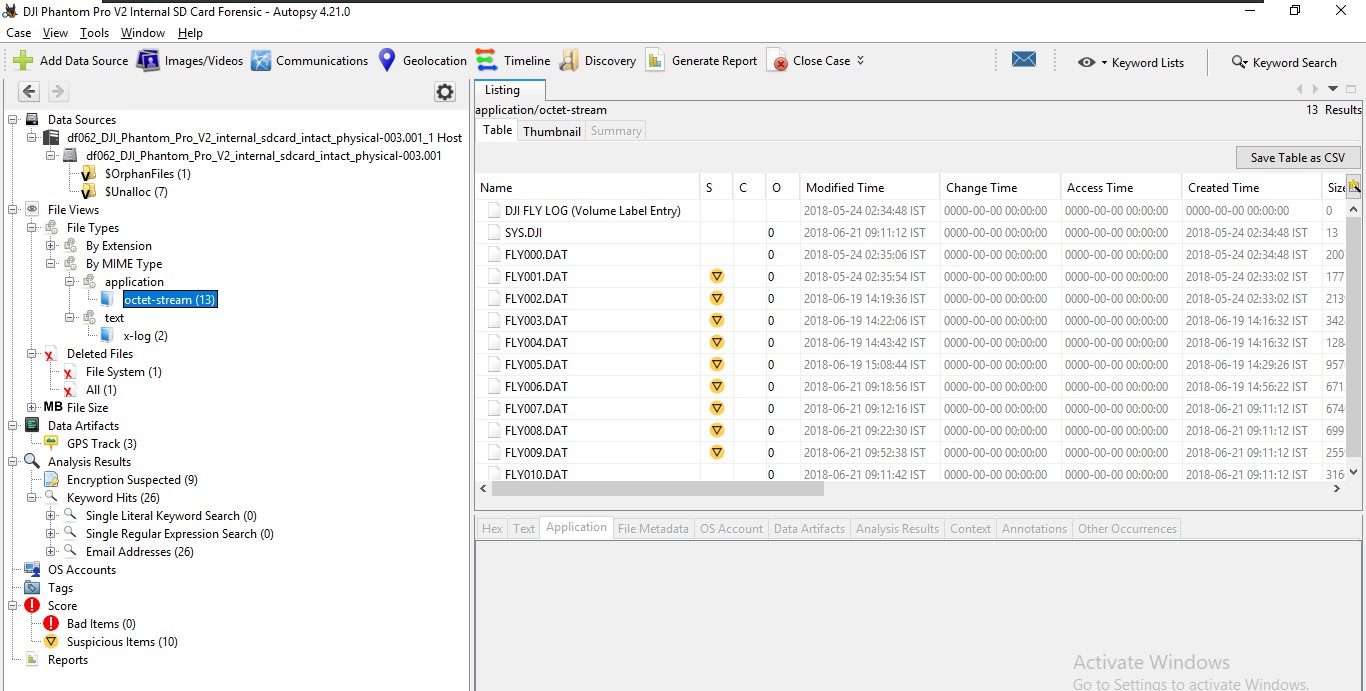
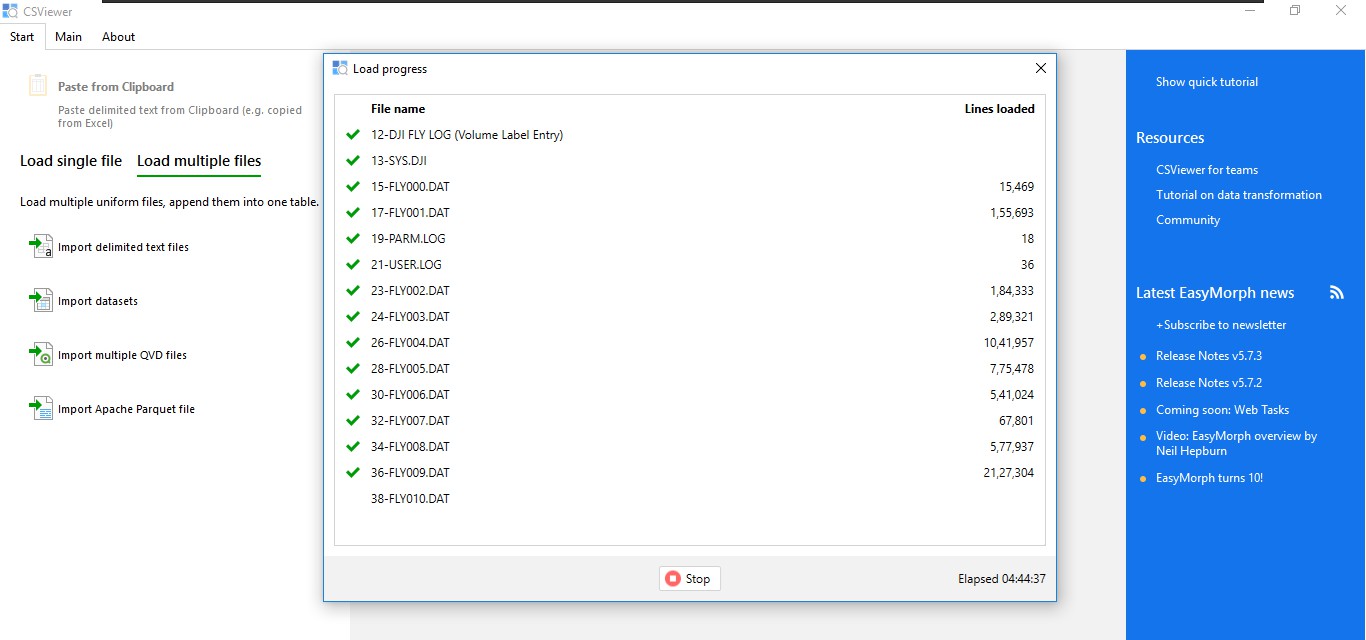
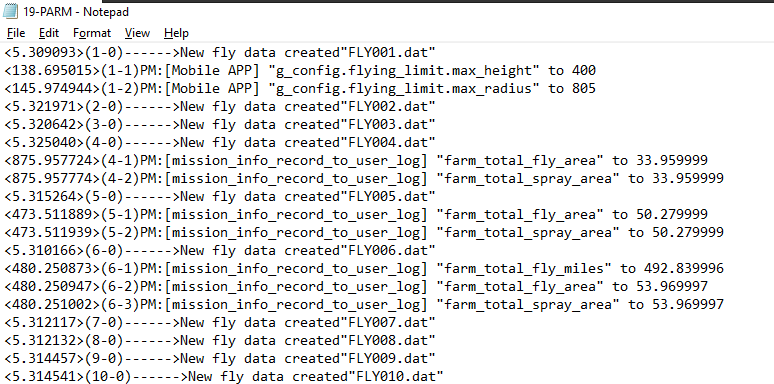


Figure ?? xxxxx

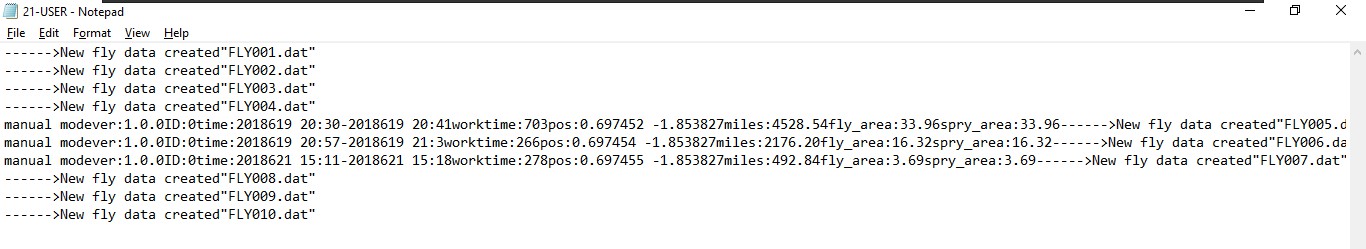
Some data was analyzed without converting it into the .csv format as shown in Figure 2.



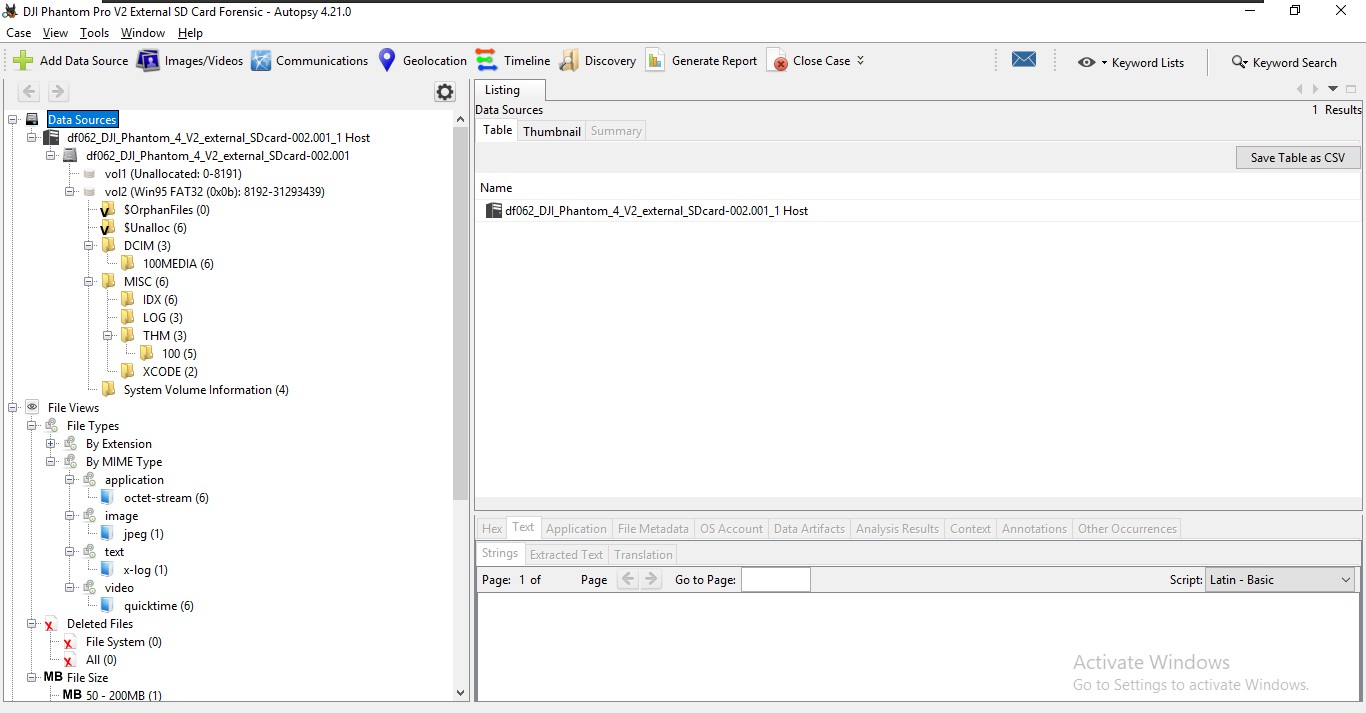
In the PARM file it contains the Flight data history as text format like creation of every flight log as ON and OFF then, which file contain the amount of data based on the flight.



The PARM file also saves the data in USER log file as “mission\_info\_record\_to\_user\_log” but in the USER file the log is saved as time, worktime, miles, position and area.

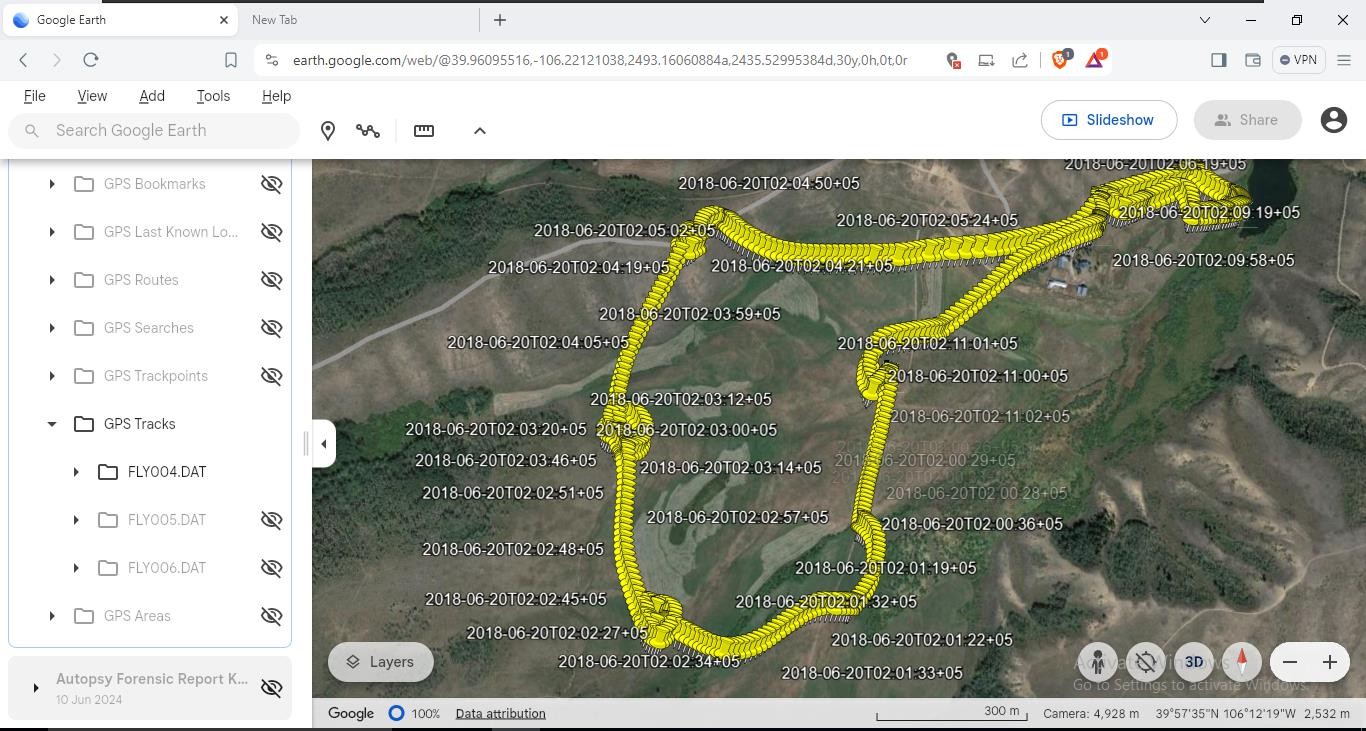


Analysis of SDCard\_external was done and it was found that some data like CameraLogCur, WPSettings.dat, IndexerVolumeGuid, some Videos and Images for extracted in a separate folder for analysis.

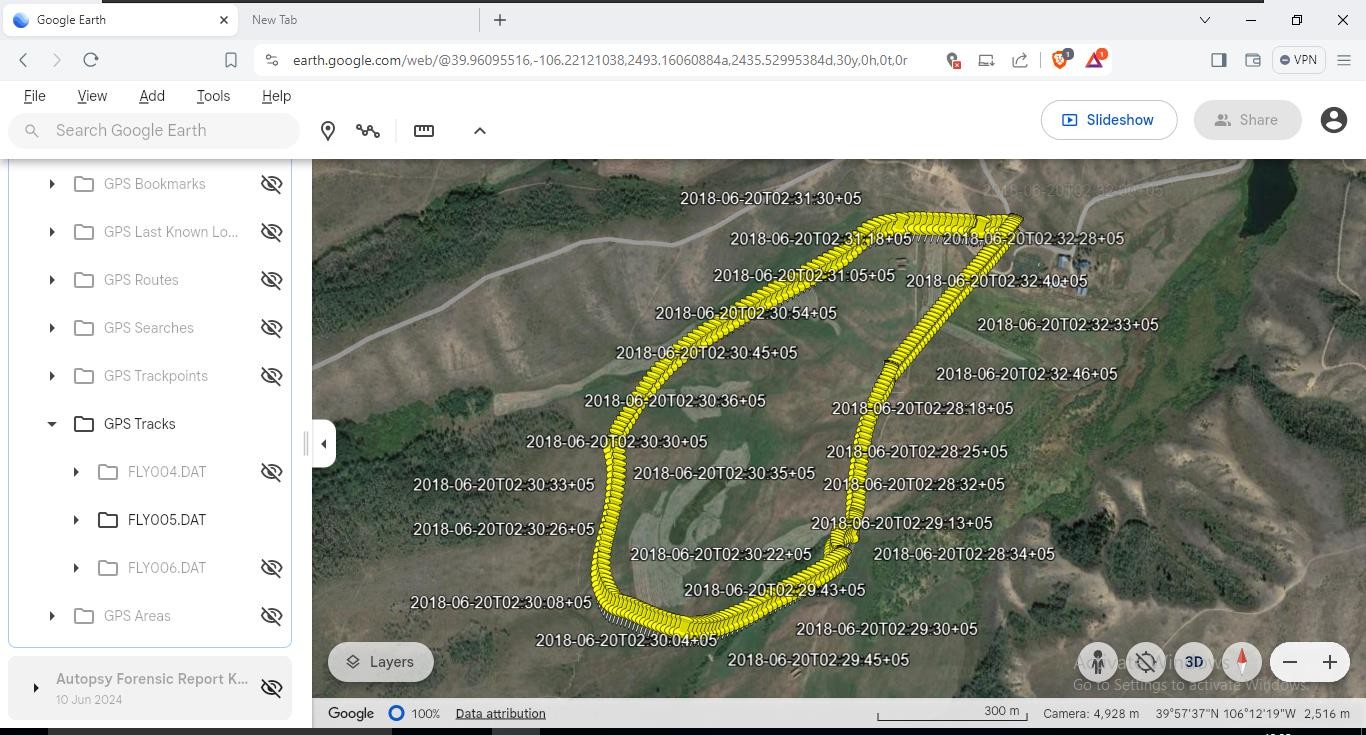


After extracting all important data i generate a report as kml file for analysis.

The internal SD card gives flight logs like it contains some FLY000.DAT etc in this only 3 file contains the useful data for analysis and these files are FLY004.DAT, FLY005.DAT, FLY006.DAT because it contains important data.



This log shows the flight data visualization stored in FLY004.DAT



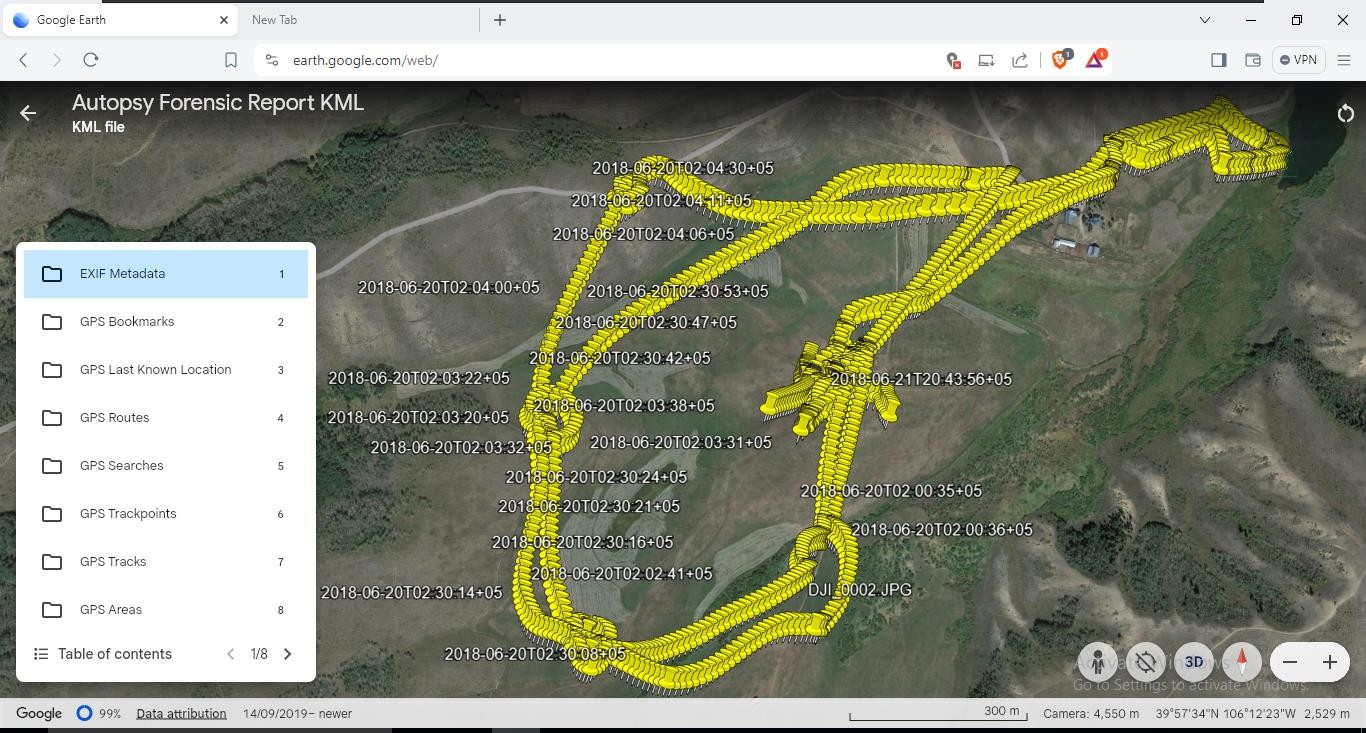
This log shows the flight data visualization stored in FLY005.DAT



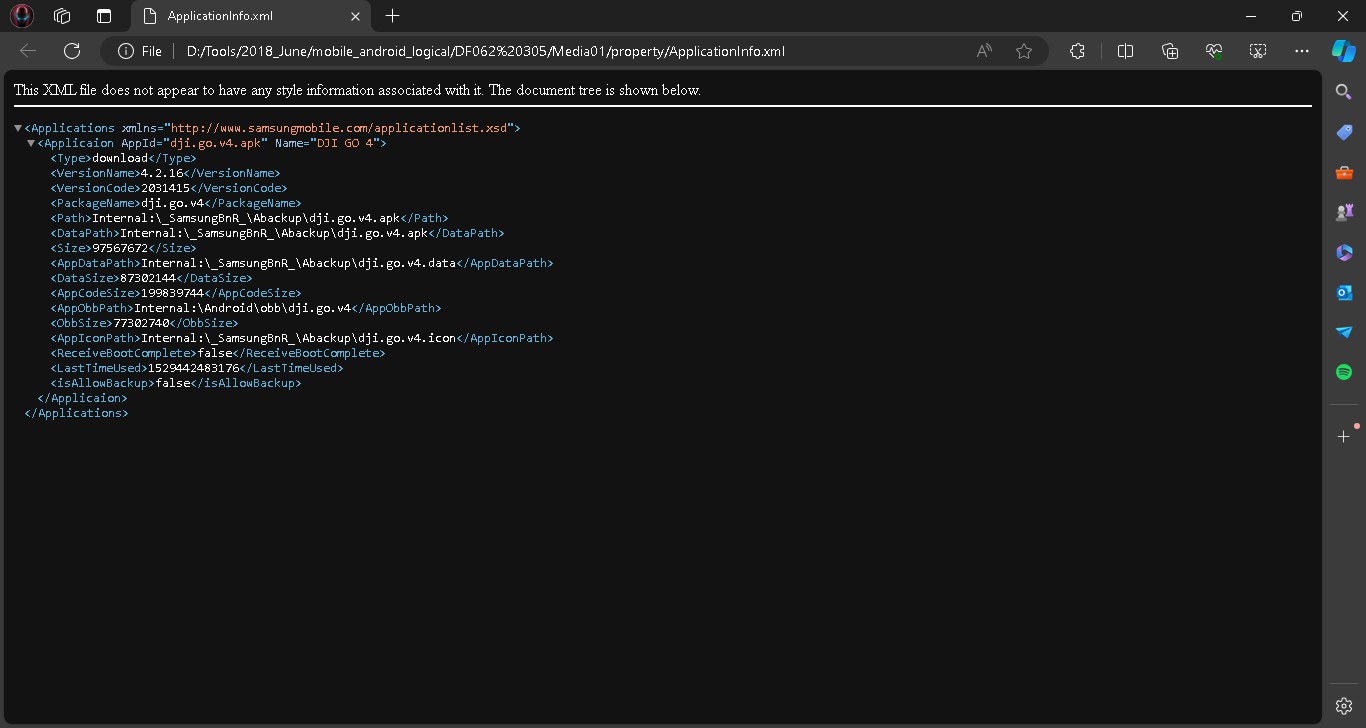
This log shows the flight data stored in FLY006.DAT

After completing all these forensics and extracting all important logs.

A Generated Report KML file of Internal and external SDCard and into Google Earth for flight log examination or visualizing all flight paths and it shows all at once in the Patterns as indicated by pinpoints.



A Collection of all the Internal and External KML files as shown



Then I do a deep analysis in Android and found out some important Application regarding data.

# CONCLUSION

The forensic analysis of the DJI Phantom 4 Pro V2.0 provides a comprehensive understanding of the drone's operational history, user interactions, and involvement in specific incidents. By extracting flight logs, media files, and application data, investigators can reconstruct the drone's

activities, uncovering detailed information about its flight paths, altitudes, speeds, and locations. This detailed data acquisition process is crucial for determining the drone's role in events such as security breaches, accidents, or unauthorized surveillance. The onboard storage, including photos and videos, offers visual evidence that can corroborate the flight data and provide additional context. Furthermore, the data from the remote controller and the DJI GO 4 app sheds light on the user’s inputs and interactions, enhancing the understanding of the drone’s behavior and any potential anomalies.

The forensic examination and interpretation of this data allow for the identification of any irregularities, such as deviations from planned routes or unexpected maneuvers, which could indicate unauthorized use or technical issues. By analyzing sensor data from the drone's IMU, barometer, and obstacle sensing systems, investigators can also gain insights into the drone’s environmental interactions and responses to obstacles. This comprehensive analysis helps form a timeline of the drone’s activities and reconstruct events with high accuracy.

Ultimately, the forensic analysis of the DJI Phantom 4 Pro V2.0 provides a robust framework for investigating incidents involving the drone. It aids in identifying responsible parties, understanding the context of the drone's operations, and ensuring accountability. This process is essential for legal investigations, security assessments, and incident resolution, offering a detailed and reliable reconstruction of the drone’s activities and contributing to informed decision-making. By leveraging the sophisticated capabilities of drone forensics, stakeholders can address concerns related to privacy, security, and safety in an increasingly drone-populated airspace.

# REFERENCES

1. 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. Multidisciplinary Digital Publishing Institute (MDPI), Jul. 01, 2023. doi: 10.3390/drones7070430.
2. F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, “A comparative uav forensic analysis: Static and live digital evidence traceability challenges,” Drones, vol. 5, no. 2, Jun. 2021, doi: 10.3390/drones5020042.
3. S. Lee, H. Seo, and D. Kim, “Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller,” Sensors (Basel), vol. 23, no. 21, Nov. 2023, doi: 10.3390/s23218934.
4. “FRAMEWORK FOR RESPONDING TO A DRONE INCIDENT For First Responders and Digital Forensics Practitioners,” 2020.
5. S. Watson, “An update on a U.S. Department of Homeland Security R&D Project Drone Forensics Acknowledgement & Disclaimer.”
6. “Civil Aviation Regulatory Landscape of Indian Drone Ecosystem red”.
7. P. Kumar Mahla, “Military Drones in India New Frontier of Warfare,” 2022. [Online]. Available: <https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf>,
8. E. Mantas and C. Patsakis, “Who Watches the New Watchmen? The Challenges for Drone Digital Forensics Investigations,” May 2021, [Online]. Available: <http://arxiv.org/abs/2105.10917>
9. H. Azhar, “Challenges and Techniques in Drone Forensics,” 2019. [Online]. Available: [https://www.dedrone.com/resources/incidents/all [10](https://www.dedrone.com/resources/incidents/all%20%5b10)]
10. A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, “Research challenges and opportunities in drone forensics models,” Electronics (Switzerland), vol. 10, no. 13. MDPI AG, Jul. 01, 2021. doi: 10.3390/electronics10131519.
11. Murdoch, Watney. (2022). Ethical and Legal Aspects Pertaining to law Enforcement use of Drones. Proceedings of the ... international conference on information warfare and security, 17(1):358-365. doi: 10.34190/iccws.17.1.27
12. Brian, T, Smith. (2016). Ethics On The Fly: Toward A Drone - Specific Code Of Conduct For Law Enforcement.
13. None, Q-A. (2023). Moralities of Drone Violence. doi: 10.1515/9781474490108.
14. Ihor, Yefimenko. (2022). Unmanned aerial vehicle as a forensic technical tool and object of forensic research. Ûridičnij časopis Nacìonalʹnoï akademìï vnutrìšnìh sprav, 12(4) doi: 10.56215/04221204.61.
15. Melissa, Beauregard., Nathan, P., Mayercsik., RA, Pietersen. (2022). A Critical Assessment of Unmanned Aerial System Usage and Data Analysis in Forensic Assessment. Forensic engineering, doi: 10.1061/9780784484548.056.
16. Elhaam, Debas., Abdullah, Albuali., M., M., Hafizur, Rahman. (2024). Forensic Examination of Drones: A Comprehensive Study of Frameworks, Challenges, and Machine Learning Applications. IEEE Access, 1-1. doi: 10.1109/access.2024.3426028.
17. Fahad, E., Salamh., Mohammad, Meraj, Mirza., Umit, Karabiyik. (2021). UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies. Electronics, 10(6):733-. doi: 10.3390/ELECTRONICS10060733.
18. Ziyu, Zhao., Yongquan, Wang., Genwei, Liao. (2024). Digital Forensic Research for Analyzing Drone and Mobile Device: Focusing on DJI Mavic 2 Pro. Drones, 8(7):281-281. doi: 10.3390/drones8070281
19. Maryam, Yousef., Farkhund, Iqbal., Mohammed, Hussain. (2020). Drone Forensics: A Detailed Analysis of Emerging DJI Models. 066-071. doi: 10.1109/ICICS49469.2020.239530
20. Aaron, Taylor. (2023). A Digital Forensics Case Study of the DJI Mini 3 Pro and DJI RC. arXiv.org, abs/2309.10487 doi: 10.48550/arxiv.2309.10487
21. Alan, Roder., Kim-Kwang, Raymond, Choo., Nhien-An, Le-Khac. (2018). Unmanned Aerial Vehicle Forensic Investigation Process: DJI Phantom 3 Drone As a Case Study. arXiv: Cryptography and Security,
22. Argyrios, Georgiou., Peter, Masters., Stephen, Johnson., Luke, Feetham. (2022). UAV‐assisted real‐time evidence detection in outdoor crime scene investigations. Journal of Forensic Sciences, 67(3):1221-1232. doi: 10.1111/1556-4029.15009
23. A., Pathania., D., P., Gangwar., Shivanshu., Poonam., Arpita. (2021). Unmanned Aerial Vehicle Forensic Investigation Process : Dji Phantom 4 Drone as A Case Study. International Journal of Scientific Research in Science and Technology, 593-599. doi: 10.32628/CSEIT2174136
24. Siniša, Husnjak., Ivan, Forenbacher., Dragan, Peraković., Ivan, Cvitić. (2022). UAV Forensics: DJI Mavic Air Noninvasive Data Extraction and Analysis. 115-127. doi: 10.1007/978-3-030-67241-6\_10
25. Ravin Kumar, Animesh Kumar Agrawal, Drone GPS data analysis for flight path reconstruction: A study on DJI, Parrot & Yuneec make drones, Forensic Science International: Digital Investigation, Volume 38,2021, doi.org/10.1016/j.fsidi.2021.301182
26. <https://cfreds.nist.gov/all/SteveWatson%2FVTOInc./DroneDataSet>
27. https://www.flightreader.com/