NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

**NFSU – Journal of Cyber Security and Digital Forensics**
**Volume – 2, Issue – 2, December 2023**
**E – ISSN – 2583-7559**

# ARTIFACTS RECOVERY METHODS AND ITS CHALLENGES IN DIFFERENT MODELS OF DRONE

***Akanksha Yadav[1], Kapil Shukla[2], Krishna Modi[3]***

*Student[1] of School of Forensic Sciences,*
*Specialization in Cyber Forensics*

*TRA[2,3] of School of Forensic Sciences*
*National Forensic Sciences University*
*National Forensic Sciences University*
*Gandhinagar, Gujarat, India*
*Email id – akankshayadav1811@gmail.com*
*Gandhinagar, Gujarat, India*

**Abstract-This paper focuses on drone forensic which is an emerging field. The crimes related to drone are increasing day by day because the demand of drone is increasing in almost every field. So it is very important to focus on digital evidences of drone, how to extract data from it & analyze that what kind of artifacts present in different models of drone. This work includes the analysis of collected data to find out that which kinds of data are found in different models of drone & also revealing the encrypted data inside them by the use of different forensic tools & softwares.**

**Keywords: Drone, drone forensics, UAV (Unmanned Aerial Vehicles), propeller, gyroscope, SSID(Service Set Identifier), CSV view, DatCon, FTK imager, autopsy, write-blocker device, EXIF tool, winhex editor**

## I. Introduction

Nowadays, we are very familiar with **UAV (Unmanned Aerial Vehicles)** which is frequently known as **drone** because it is utilized for various purposes such as communication, wildlife monitoring, emergency rescue, photography, disaster response, geographic mapping protection, border control surveillance, military etc [10, 12, 13, 14].

But it comes to highlight when we are talking about involvement of drones in crime commission which is a serious problem in this era & need to concern about it. The crime cases related with drones increased because it is easily accessible & cost-effective also. The low price of drones will make all type of users to purchase it, especially criminals for their illegal motive. With the help of drone, people are involved in dangerous crimes which results in threat to life, property, mind & even to the national safety & security.

There is need to realize the importance of drone forensic because this field is not so familiar for law enforcement agencies & digital forensic investigator as compared to other fields. Whenever a case comes in front of a court, it is very crucial to detect & find the evidences from UAV which is suspected to used for illegitimate purpose. The seized UAV device can reveal rich sources of uncompromised digital data which can be used as an evidence in civil as well as criminal cases. Proper identification, extraction, acquisition, preservation & analysis of important artifacts from SD card, remote controller & mobile which are used to operate the drone by the application of forensic tools & techniques. The involvement of forensic in analysis of drone evidences provides a lot of information which is helpful to apprehend the suspects [15, 16].

## II. Related Work

The field of drone forensics comes to highlight because drones are using in crime commission such as smuggling, privacy breach, spying, terrorism etc. In 2011, a staff of Moscow prison seized with 700 gm. of heroin dropped by drone .In 2016, prison of oklahoam discovered drones dropping drugs, mobile phones, blades of hacksaw & other items. In 2015, an incident happened in White House Lawn in which a drone crashed, may be used by terrorist to capture the photos by the use of drone camera [5].

The crime commission by drone is increasing day by day, so the involvement of forensics in analysis of drone is necessary by following the investigative procedure. An investigator should have knowledge about the hardware & firmware of UAV devices, have skills to detect any kind of alterations. The proper collection of volatile data, non-volatile data, data from removable media evidences. Always use a write blocker at the time of collecting data to avoid modification & addition of data in digital evidence. Maintain the integrity of data by creating the hash value of data which shows that the data found in the UAV digital device is not altered or modified. It is necessary to perform investigation process on working copy of original evidence. Analyze the data by the use of software tools. After the analysis & result, a report should be prepared to present the case details, evidences, its examination & result in court. It should be simple & understandable for judges & jury members in court [3].

The crucial data of drone can be extracted from mobile phone, SD card of drone, remote controller. A mobile phone is also used to operate drone by the help of apps such as DJI GO app, free flight 3 app etc. These digital evidences provides a lot of data such as flight records in dat, txt, pud

format, media files (photos, videos), serial number of remote controller, location, height, battery voltage, landing sequence, hardware & software events of UAV etc. [1, 2, 4, 5, 6, 11].

Different software tools are used to analyze data such as FTK imager, autopsy, EXIF tool kit, Csv view software, winhex editor, DJI viewer, DatCon. Autopsy is used to explore flight record data within the directory & it helps to decode the encrypted flight data. It also extracts photos, videos, media files. EXIF Tool kit is used to read the EXIF header of the image. Csv view is a software which converts the DAT & TXT files into CSV (comma-separated values). DJI log viewer & DatCon are also used to open the DAT & TXT files to analyze the flight data & converts them into readable .csv file [1, 2, 4, 5, 9, 17].

## III. Methodology

This work included the collection & analysis of drone datasets with the aim of finding that which kinds of data are found in different models of drone to compare them. It is also aimed at revealing the hidden data by the use of tools.

The datasets of drone collected form NIST (National Institute of Standards & Technology). The information of NIST drone datasets got from the website – NIST Builds Drone Forensic Datasets for Law Enforcement of DSIAC (Defence System Information Analysis Center). This website provided in detail that where to look for datasets & how to get it. This website also mentioned that the NIST included forensic images of 14 popular makes & models of drone in its CFReDS (Computer Forensic Reference Datasets) for law enforcement agencies to extract information.

The NIST CFReDS website provided the datasets of different makes & models of drone. In this website, there were a lot of datasets provided other than drone datasets. There was an URL link in the page of drone dataset through which the datasets were downloaded. After that the datasets were started downloading & automatically saved in drive [7,8].

In the drive of drone forensic dataset, there were dataset of 30 drone models in separate folders. There were datasets of 2-3 drone devices in each folder of a drone model. The folder of each drone device contained data of year 2017 & 2018. There were data of SD card of camera & aircraft, backups of iOS & android mobile phones, remote controller, zip files of flight logs, image files.

## IV. Analysis & Result

After the completion of data collection, the analysis of collected data started. The analysis part covered the examination of important artifacts, what kinds of data are present & where to look for these kinds of data. Two models of drone – DJI Phantom 4 & Yuneec Typhoon were chosen from 30 different models of drone because they both are widely used models of drone.

### A. DJI Phantom 4

The folder of DJI Phantom 4 contained datasets of 3 drone devices (df0004_DJI_Phantom_4, df0005_DJI_Phantom_4, df0006_DJI_Phantom_4, ) from which any one device was chosen for analysis. The device df0005_DJI_Phantom_4 contained datasets of two years – 2017 & 2018. The folder of 2017 dataset contained the data of SD card, iOS & android mobile, image files. The folder of 2018 contained the data of iOS mobile, flight logs & image files. Downloaded all the datasets which were found & saved them in computer.

The downloaded datasets were examined & analyzed properly to find out the different kinds of data & where they are present. There were image files, zip files of iOS & android mobile. The zip file of android mobile is represented in figure 1a, 1b & 1c. The zip file of iOS mobile is represented in figure 2.

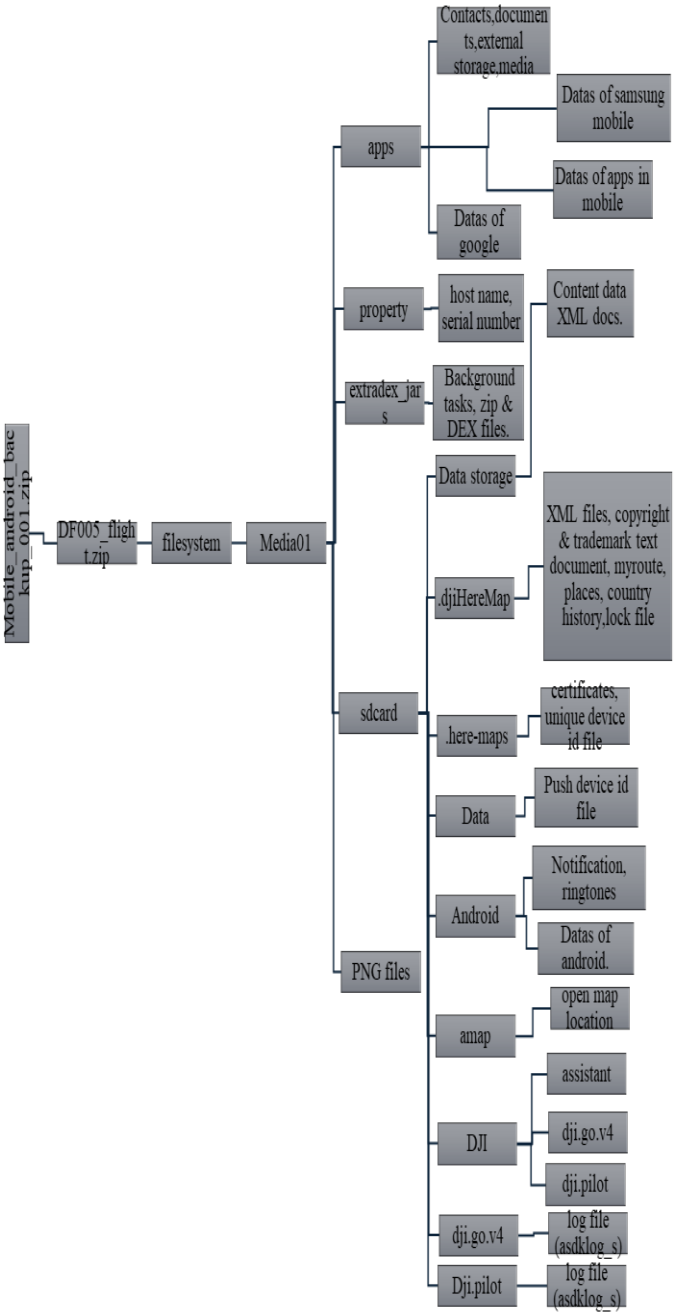



**Fig. 1a - The structure of android zip file**

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

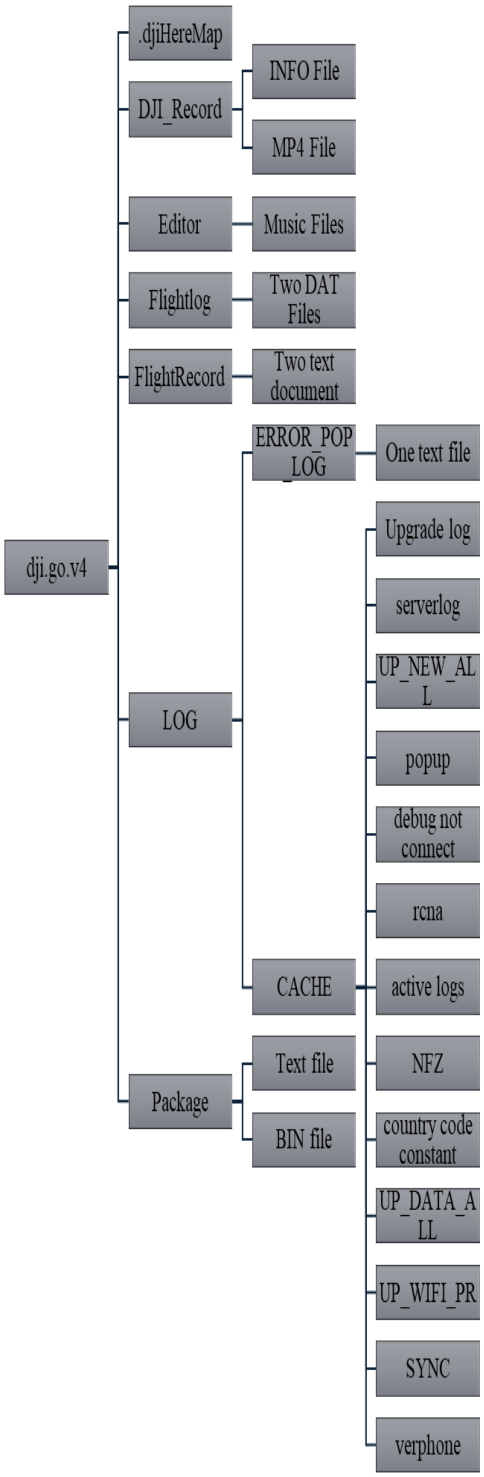



**Fig. 1b – The structure of dji.go.v4 of android zip file**

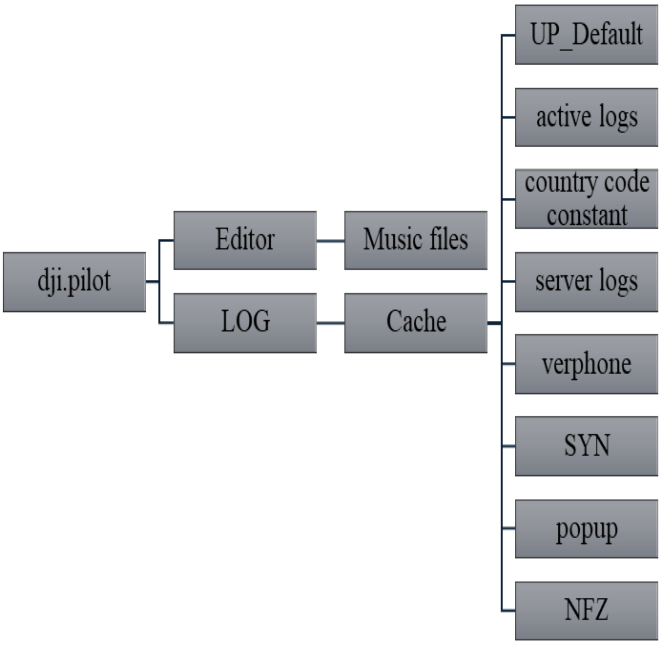



**Fig. 1c – The structure of dji.pilot of android zip file**

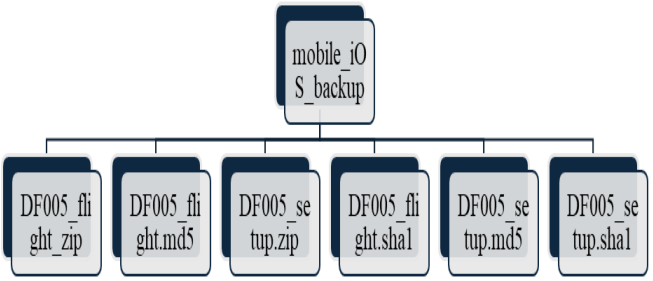



**Fig. 2 – The structure of iOS mobile zip file**

**B. Yuneec Typhoon Q500 4k**

The folder of Yuneec Typhoon Q500 4k contained datasets of 3 drone devices (df028_Yuneec_Typhoon_Q500_4K,df029_Yuneec_Typhoon_4K,df030_Yuneec_Typhoon_4K) from which any one device was chosen for analysis. The device df028_Yuneec_Typhoon_Q500_4K contained datasets of two years – 2017 & 2018. The folder of 2017 dataset contained data of controller micro SD card, camera SD card, image files. The folder of 2018 contained the data of controller SD card, camera SD card, controller logical file, image files. Downloaded all the datasets which were found & saved them in computer.

The downloaded datasets were examined & analyzed properly to find out the different kinds of data & where they are present. There were image files, zip file of controller micro SD card which contained only one E01 file, zip file of controller logical. The zip file of controller logical is represented in figure 3a, 3b, 3c.

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

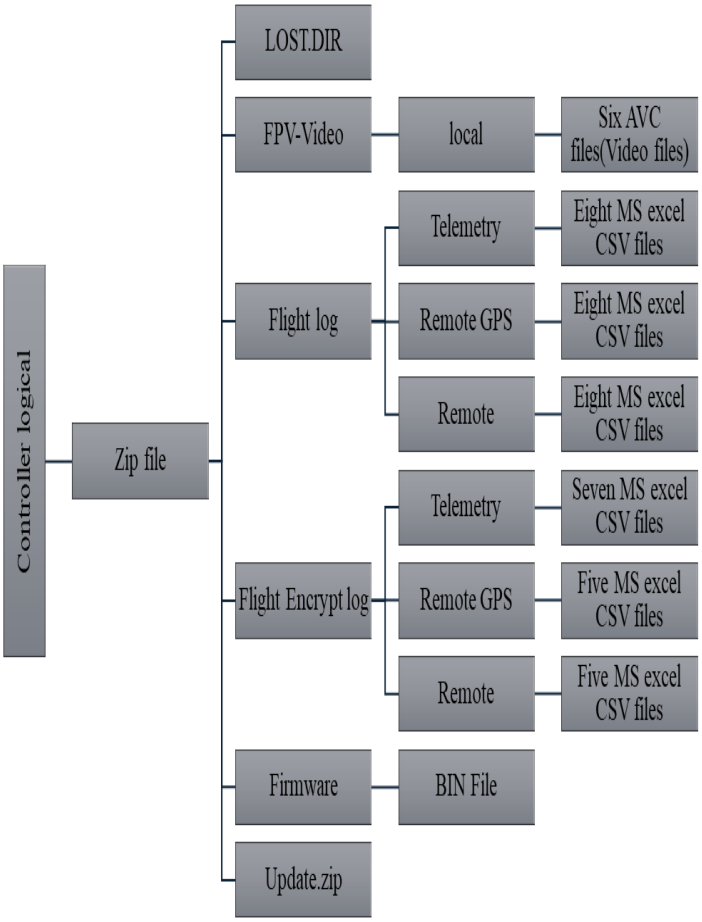



**Fig. 3a - The structure of controller logical zip file**

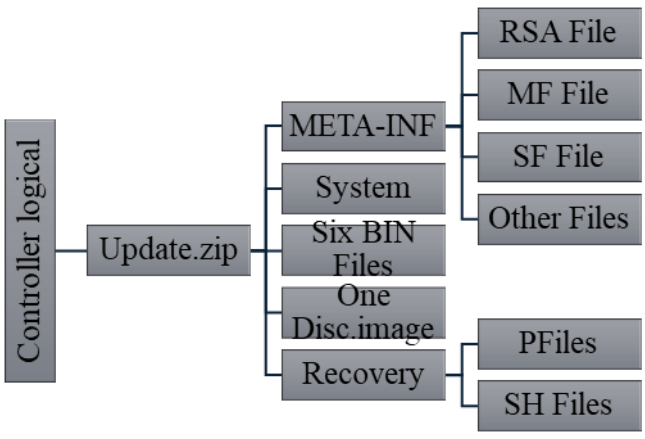



**Fig. 3b - The structure of update.zip of controller logical zip file**

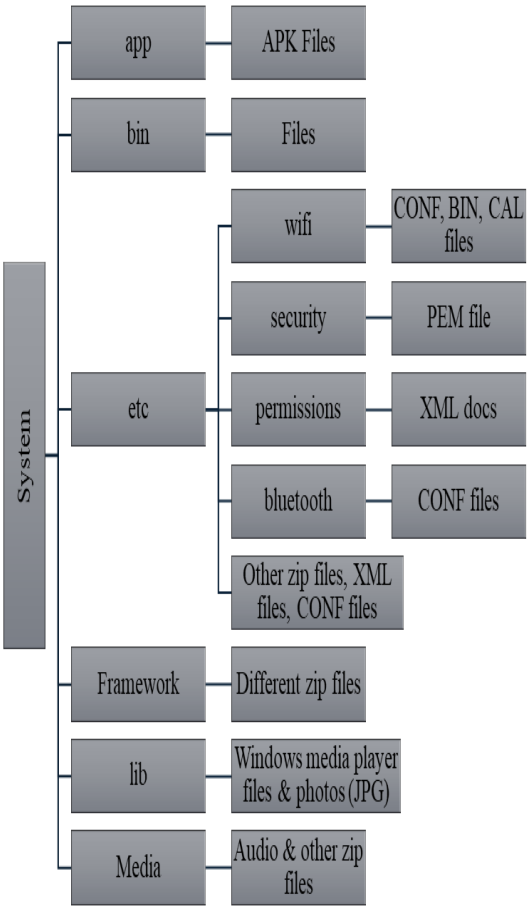



**Fig. 3c - The structure of system of controller logical zip file**

The data found from different models of drone were compared & it is shown in table 1.

**Table 1 – Comparison of DJI Phantom 4 data & Yuneec Typhoon data**

| **Data retrieved from DJI Phantom 4** | **Data retrieved from Yuneec Typhoon** |
|---|---|
| The data retrieved from mobile phones. | The data retrieved from controller of drone. |
| In this, the mobile phones provided all information that was present in SD card of drone as well as in mobile devices. | In this, only remote controller provides data because there was no mobile data found. |
| It contained flight records in DAT & TXT files. | It contained flight records in MS excel CSV files. |
| It had all flight records in encrypted form. | It had flight records in plain text as well as in encrypted form. |

## V. Retrieval of Hidden data

It is very important to recover the hidden data because they can reveal a lot of facts. Here, it was mainly focused on GPS coordinates which were hidden in DAT files of flight records to get the flight details followed by drone. Autopsy & FTK imager tools both were used to retrieve the hidden GPS coordinates.

At the time of process, the DAT file was not able to save in the computer, so copied the written material in notepad &

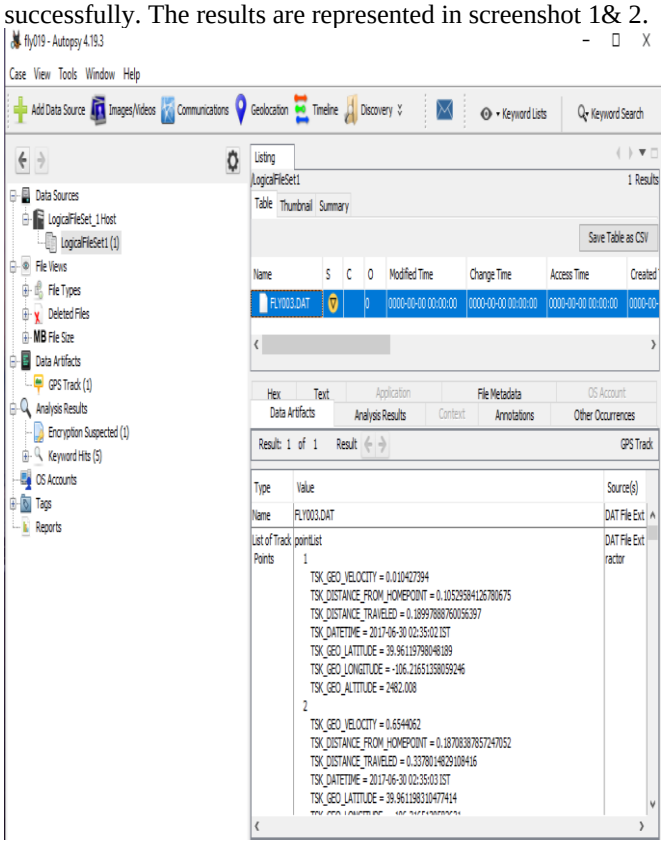
NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

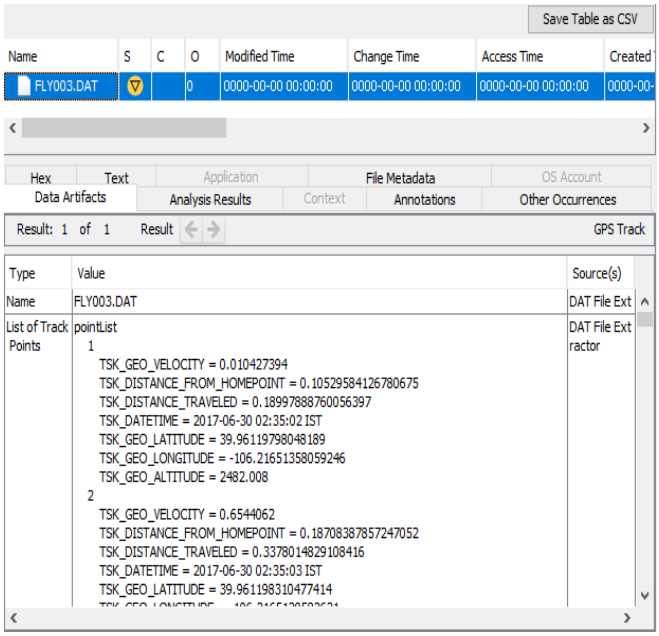
saved it as fLY019. Then uploaded the fly019 file in both the tools one by one.

**A. Autopsy**

The fly019 file was uploaded in autopsy after filling the necessary details & adding the data source. It showed the hidden GPS coordinates which were encrypted in DAT file successfully. The results are represented in screenshot 1& 2.




**Screenshot 1**




**Screenshot 2**

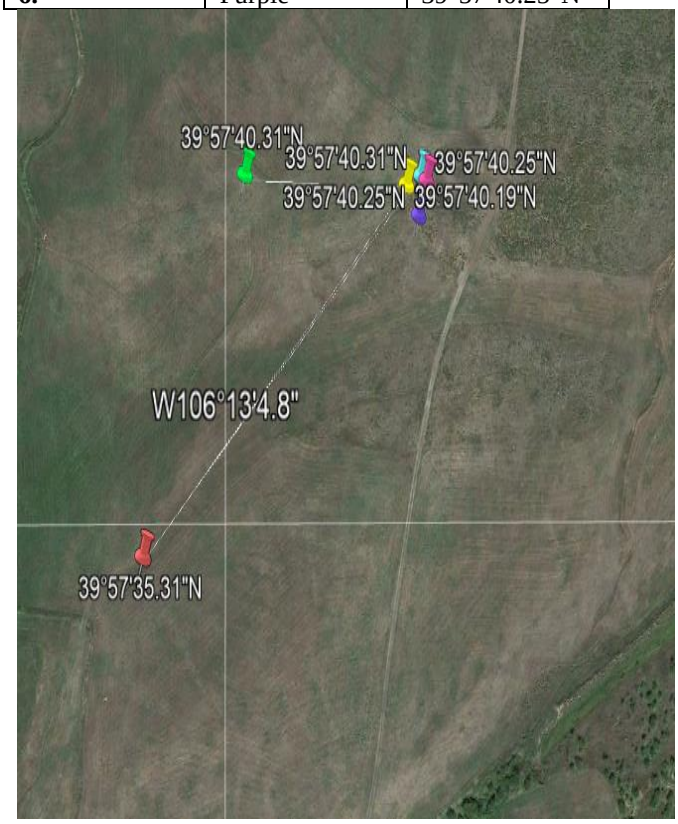
**1. Plotting of GPS coordinates on Google Earth Pro**

There were total 612 GPS coordinates recovered from DAT file by the use of autopsy. Plotted the GPS coordinates to get the path which was followed by drone through the use of google earth pro. The GPS coordinates were very close when they were plotted in Google earth pro app. So instead of plotting the near coordinates, plotted the far GPS coordinates to better understand the path which was followed by drone.

Selected the GPS coordinates in the range of 100, 200, 300, 400, 500, 600 & plotted them on the google earth pro. The GPS coordinates with their placemark are represented in table 2.

**Table 2 – GPS Coordinates with their Placemark**

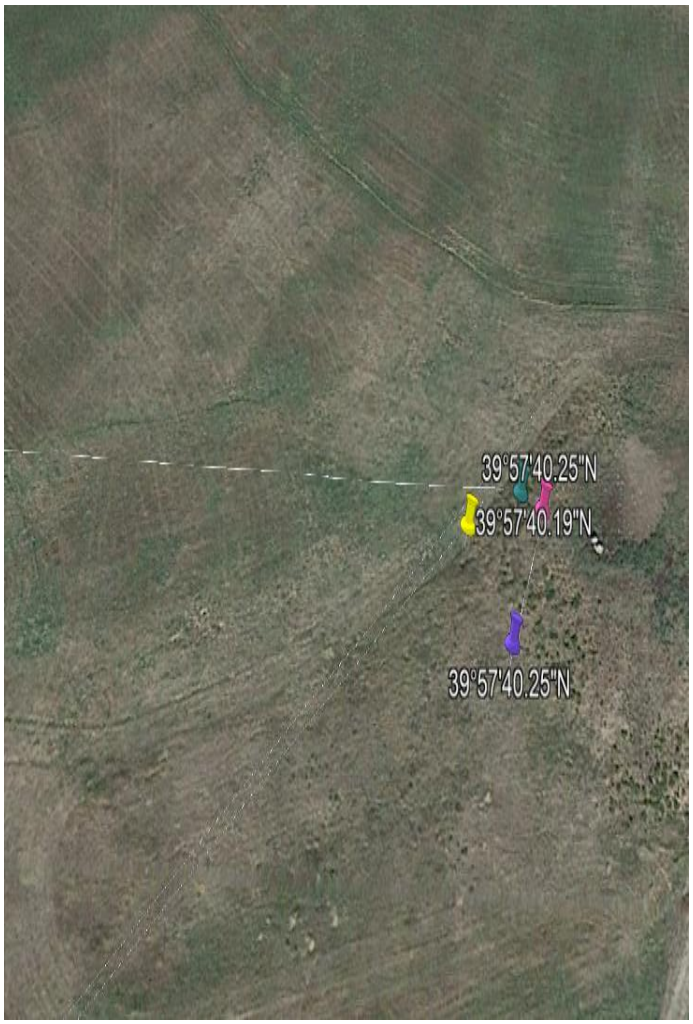
| S.No. | Placemark | GPS Coordinate |
|---|---|---|
| **1.** | Green | 39°57'40.31"N |
| **2.** | Yellow | 39°57'40.19"N |
| **3.** | Red | 39°57'35.31"N |
| **4.** | Blue | 39°57'40.31"N |
| **5.** | Pink | 39°57'40.25"N |
| **6.** | Purple | 39°57'40.25"N |




**Screenshot 3**

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

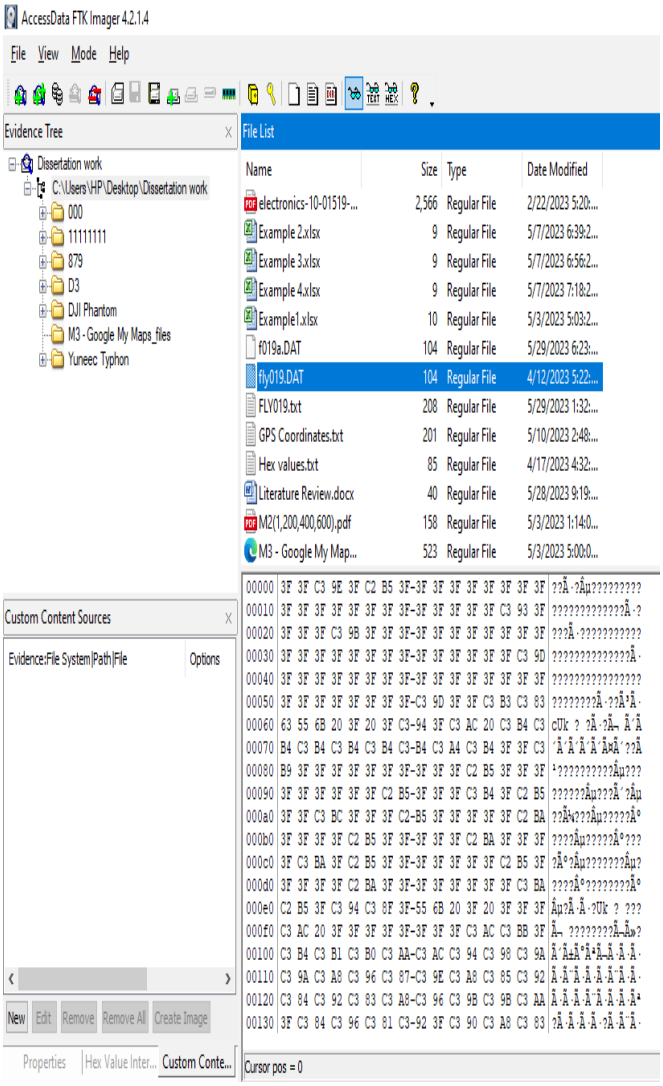
**NFSU – Journal of Cyber Security and Digital Forensics**
**Volume – 2, Issue – 2, December 2023**
**E – ISSN – 2583-7559**




Screenshot 4

**B. FTK Imager**

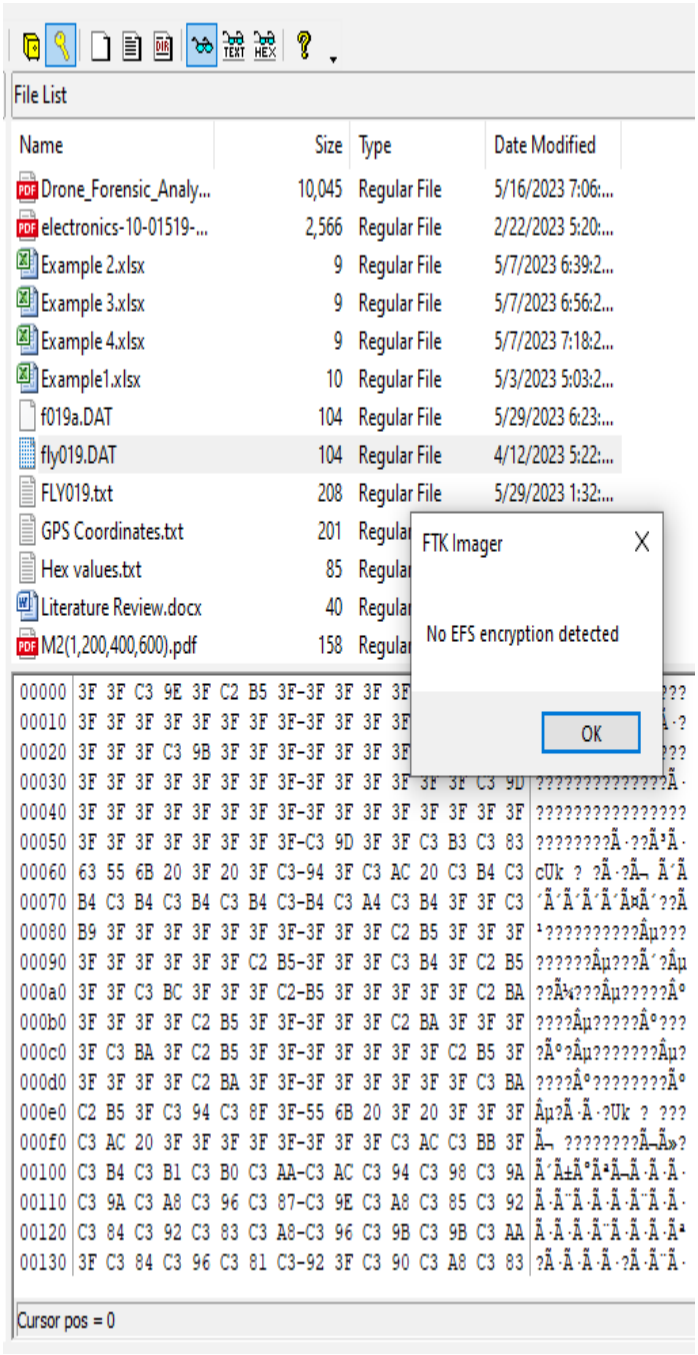
The fly019 file was uploaded in FTK Imager after filling the necessary details, adding the evidence item & source path. It showed the data in hex values but it was not able to recover the encrypted data inside the DAT file. The results are represented in screenshot 5 & 6.




**Screenshot 5**

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

**NFSU – Journal of Cyber Security and Digital Forensics**
**Volume – 2, Issue – 2, December 2023**
**E – ISSN – 2583-7559**



Screenshot 6

## VI. Conclusion

The field of drone forensic is still emerging. The work in this paper provides the detailed knowledge of data present in DJI Phantom 4 & Yuneec Typhoon which shows little difference in their artifacts. The tools which were used to analyze the data especially hidden data, detect by only one tool (Autopsy) & other tool (FTK imager) was not able to detect the hidden data. So it is necessary to focus & explore the reason behind that why FTK Imager was not able to detect the encrypted data. There should be more tools required to detect these kinds of important artifacts because it is very necessary to uncover the real truth in criminal cases.

## VII. References

**[1]** Llewellyn, M. (2017). "DJI Phantom 3 – Drone Forensic data exploration", Edith Cowan Univ., Perth, Western Australia.

**[2]** Azhar, M A H. B., Barton, T. E A., Islam T. (2018). "Drone Forensic Analysis Using Open Source Tools in The Journal of Digital Forensics, Security and Law", Dept. of Computing, Digital Forensic & Cyber Security, Canterbury Christ Church Univ., Canterbury, United Kingdom.

**[3]** Gulatas, I. (2018). "Unmanned Aerial Vehicle Digital Forensic Investigation", Master's Thesis, Dept. Comp. Engr., The Republic of Turkey Bahcesehir Univ.

**[4]** Kao, D., Chen, M., Wu, W., Lin, J., Chen, C., Tsai, F. (2019)"Drone Forensic Investigation : DJI Spark Study as A Case Study", Dept. Info. Mgmt., Central Police Univ., Dept. Criminal Investigation, Central Police Univ., Dept. New Taipei City Police, New Taipei city, Taiwan.

**[5]** Iqbal, F., Al-Room, K., Shah, B., Baker, T., MacDermott, A., Yankson, B., Hung, P. C.K. (2021). "Drone Forensics : A Case Study of Digital Forensic Investigations Conducted on Common Drone Models", Zayed Univ., UAE, Liverpool John Moores Univ., UK, Univ. of Ontario Institute of Technology, Canada & Sheridan Coll., Canada.

**[6]** Bouafif, H., Kamoun, F., Iqbal, F., Marrington, A. (2021). "Drone Forensics : Challenges and Insights", Holy Spirit Univ. of Kaslik, ESPRIT, Zayed Univ., UAE.

**[7]** DSIAC. (2018, July 30). NIST Builds Drone Forensics Datasets for Law Enforcement Agencies [Online]. Retrieved May 1, 2023, from https://dsiac.org/articles/nist-builds-drone-forensics-dataset-for-law-enforcement/

**[8]** CFReDS. (n.d.). Drone Data Set [Online]. Retrieved May 1, 2023, from https://cfreds.nist.gov/

**[9]** Suryadithia, R., Pangesti, W. E., Faisal, M., Nurrohman, A., Wibisono, Putra, A. S. (2022). "FTK Image For Forensic Data Processing In Forensic Tools", Faculty of Engineering and Informatics, Bina Sarana Informatika Univ., Faculty of Information Technology, Nusa Mandiri Univ., Faculty of Informatics, Institut Teknologi Budi Utomo, Faculty of Information System, STMIK Insan Pembangunan.

**[10]** UAV. (2018). Tarot T-18 Ready To Fly Drone I U AV Systems International. Retrieved 23 March 2018, from https:// www.uavsystemsinternational.com/ product / tarot-t-18-ready-fly-drone /

**[11]** DJI. (2018). Phantom 3 Professional - Specs, FAQ, Tutorials, Downloads and DJI GO - DJI. Retrieved 23 March 2018, from https: // www.dji.com/ phantom-3-pro / info# specs

**[12]** Sivakumar, M., TYJ, N. M., "A Literature Survey of Unmanned Aerial Vehicle Usage for Civil Applications", Dept. of Networking & Communications, SRM Institute of Science and Technology, Chennai/Tamilnadu, India, 2021.

**[13]** Hossain, R. "A Short Review of the Drone Technology", Research Student, Dept. Eng., National Univ., Kushtia Govt. Coll., Kushtia, Dhaka Bangladesh, 2022.

**[14]** Zanero, S., & Huebner, E. (2010). The Case for Open Source Software in Digital Forensics. In Open Source

Software for Digital Forensics (pp. 3- 7). Boston, MA: Springer US. https://doi.org/10.1007 /978-1-4419-5803-71.

**[15]** Årnes, A. (2018) Digital Forensics. Wiley, J. & Sons Ltd.

**[16]** Jones, G.M. and Winster, S.G. (2017) "Forensics Analysis on Smart Phones Using Mobile Forensic Tools. " International Journal of Computational Intelligence Research (13) 8: 1859-1869.

**[17]** Csv. (2017). CsvView Downloads. Retrieved 24 March 2018, from https://datfile.net/Csv View/downloads.html