International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2174136

Unmanned Aerial Vehicle Forensic Investigation Process : Dji Phantom 4 Drone as A Case Study

A. Pathania*, D. P. Gangwar, Shivanshu, Poonam, Arpita Angrish
Central Forensic Science Laboratory, Physics Division, Chandigarh, GOI, DFSS, MHA , India
*Corresponding Author: pathania.anju83@gmail.com

Article Info
Volume 7, Issue 4
Page Number : 593-599

Publication Issue :
July-August-2021

Article History
Accepted : 12 Aug 2021
Published : 23 Aug 2021

ABSTRACT

A drone, technological term Unmanned aerial vehicle (UAV), means any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board. Essentially, a drone is a flying robot that can be remotely controlled or fly autonomously through software-controlled flight plans in their embedded systems, working in conjunction with onboard sensors and GPS. The easy accessibility to everyone led to an increase in drone crime. Criminals are using drones in many malicious activities worldwide due to the drones' ability to offer live-stream, real-time video, and image capture, along with the ability to fly and transport goods. Terrorist groups are using aerial drones to conduct and coordinate attacks. Forensic laboratories have been receiving Drone cases throughout India. The drone has been built that can be operated by a radio frequency controller and send live audio-visual feedback. This paper aims to provide a case study of Drone, DJI Phantom 4 and presents the acquisition, examination, analysis of important artifacts recorded flight data and discuss some possible data extractions from its flash memory, GPS (navigator) & SD card.

Keywords : Drone forensics, UAV forensics, forensic challenges, forensic case study.

I. INTRODUCTION

Drones are known as Unmanned Aerial Vehicles (UAV). Drone technology is not only confined to use in the military, entertainment industry, and meteorology, due to its easy accessibility, it is also widely used by the public. A drone is a remotely controlled aircraft that is capable of capturing images and videos of a targeted area. A drone is usually controlled by a handheld device such as a radio controller, a mobile phone, or a tablet [1]. UAVs are being used by terrorists and other miscreants to launch illegal actions, to spy on the

privacy of citizens, sensitive places and nation-states, to smuggle contraband items, and the unauthorized launching of aerial terrorist attacks. In this case, the drone has been caught in intended violation of no-fly zones, instances of which are growing day by day. The potential misuse of drones to launch illegal or criminal activities led forensic analysts to pay increased interest in exploring the forensic aspects of these devices. Traditionally, digital forensics has focused on extracting evidence from conventional computing devices such as mobile phones, computers, tablets, or digital cameras because the pervasive usage of these devices makes them more likely to be used by criminals [2]. In this study, we investigate and present the results of a forensic analysis performed on an exhibit-Drone DJI Phantom 4. We present our methodology to conduct a forensic analysis on drones, important experimental results on the DJI Phantom 4, and a summary of the key findings of this study. After seizing the drone, a forensic analysis can provide a lot of information about the potential suspect of a crime based on the data gathered from onboard sensors and other electronics that assist with flight and navigations, as well as the camera and digital storage.

II. Basic Structure and its components

A UAV consists of the following components:

1. Physical Components
2. Software

1. Physical Components: The physical components of a UAV constitute its body and flight mechanism. It can be broken down into the following categories:

i) *Drone Body:* It is the core structure of a UAV which contains all other components.

ii) *Motors, Rotors/Propellers/Wings, and Speed Controllers:* These parts altogether provide the lift and propulsion for the UAV.

iii) *Flight Controller:* Used to control flight and stabilize the UAV, and generally accept navigation input from a radio control device. In many systems, the flight controller can be controlled real-time from a remote location and be pre-programmed for autonomous flight.

iv) *GPS Receiver:* It is not necessarily present in all UAVs, but is common in the leading solutions. This component is used to manage UAV position, return back, and find autonomous flight routes.

v) *Radio Receiver (RX):* Used to receive control input signals from the ground-based transmitter.

vi) *Protective Casing:* This protection covering strongly encases the motors and propellers to prevent collision and loss of control, and damage to the system.

vii) *Transmitter (TX):* Transmits manual input from the operator on the ground to the UAV.

viii) *LED Lights:* Some UAVs come equipped with LED lights (usually green and red) which can be used to aid the pilot in the orientation of the drone, and help other airspace users to identify the drone.

2. Software: All UAVs include an application or software that is used to control the system when it is operational. UAV software solutions can be classified into two categories:

a) Flight Management Software: This software is uploaded on the flight controller within the UAV at one end, and also within the remote control of the user at the other end. When operational, it is used to control the UAV during take-off, flight, and landing. Typical functions which are controlled by the flight management software solution include UAV flight, device stabilization, and manual navigation input.

b) Ground Control Software: This software is used to control pre-determined navigation and effectively

plan flight schedules and is best used by a pilot when the UAV is grounded in planning and preparation for flight. Ground control software additionally facilitates enhanced live monitoring to remote users other than the pilot when the UAV is in flight - either directly to their computers or smart devices such as tablets or mobile phones. Whilst offering significant innovation and supporting technical development of skills, consideration should be given to the fact that bespoke UAVs may potentially propose increased risks and more dangerous use, as they are likely to be configured with convenience and cost, rather than safety, in mind. This may result in lack of core safety features and functionality in these drones that are built into many of the leading commercial off-the-shelf systems, such as restricted area control, obstacle avoidance, and fail-safe management. These features lessen the risk to persons and property in the event of a pilot error or a system failure. While some of these proposed categorizations of UAVs can become blurred, for example – in cases where wealthy recreational users purchase higher end UAVs that are intended for commercial purposes, this categorization approach is recommended when defining UAVs and considering their respective capabilities.

III. Related work and literature review

There are similarities between UAV and mobile device forensics [4]. UAVs are similar to a mobile device as a modern or advanced GCS (ground control system) is likely to have Wi-Fi, blue-tooth, or internet connection. Therefore, there is a possibility that the device could be remotely wiped or modified. UAV forensics can also involve conventional storage media forensics [5] (e.g. memory cards) and live forensics (e.g. real-time access to a live UAV).

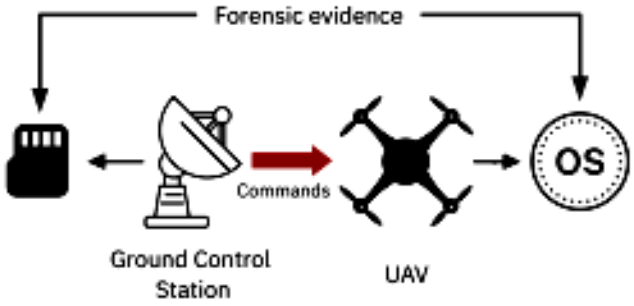

Figure 1 - Source of forensic evidence of UAVs

The existing literature is useful to guide a general forensic investigation of a UAV, having a UAV-focussed/specific forensic process that could be more useful to forensic examiners/investigators (e.g. to maintain consistency across cases).

It has been noted that there is upsurge of illegal activity involving drones including drug and weapon delivery, privacy attack, flight in controlled airspace, and flight into bystanders. In many cases, the data has been recovered which could trace the aircraft back to the owner. This included GPS and other EXIF data from pictures, launch point, DJI account information, and the owners' name.

The increased use of drones by public increases the challenges faced by digital forensic investigators. Among other findings, it has been found that drones are targeted by criminals for their payload value, data breach, and cyber-attack capabilities. Considering the past studies on drones, Roder et al. provided general guidelines for performing physical forensics and discussed some techniques for the analysis of drone-related facts by using the DJI Phantom 3 drone [7]. In 2016, a group of researchers had put forth a general overview on drone forensics by making use of the drone DJI Phantom 2. They demonstrated a sequential analysis of hardware and software components of a drone [1]. In the same year, Horsman et al. presented a preliminary forensic analysis on the Parrot Bebop UAV. The study discussed the digital analysis based on the system generated flight files, their folder structure, vehicle's operating system, and the media captured during the

flight [8]. Later in 2017, Jain et al., proposed a forensic model for determination and authentication of different components of a drone which could be used to commit illegal activities with the help of analysis of physical evidence, GPS location, and the onboard multimedia gathered from the scene of crime [9]. Apart from this, another group of researchers came forward with the utilization of the GPS coordinates of the drone for extracting the location evidence [10]. In 2018, H Bouafif et al. attempted to gather facts, file formats, etc; using the Parrot A.R Drone 2.0. [11]. Furthermore, Mhatre et al., in 2015 put forward a tool named JavaFX, for the visualization of real-time flight control [12].

IV. Case Study

In this section, we will demonstrate how our forensic process started the forensic investigation of a DJI Phantom 4 UAV (Figure 2). The hardware of the exhibit involved components that were necessary for flight and navigation.

The whole experiment was targeted at the evaluation of the data, and extraction of data/deleted data.

Figure 2- DJI Phantom 4

As this was a case exhibit, the details of the exhibit (Drone) were recorded. The make and model of the exhibit were noted down for carryig forward with the examination. They are as follows:

1. Device:
    - Model – GL300C (DJI Phantom 4)
2. Battery:
    - Model – PH4-5350mAh-15.2V
3. Video capture facility-Yes
4. Audio capture facility-No
5. Load carrying capacity-Yes
6. Exhibit components and their measurements:
    - Four propeller motors of diameter 2.8 cms
    - Diagonal length of the drone-16 inches
    - Height of the drone-7 inches
    - Eight detachable fans of the same size-24 cms
    - Camera – DJI, F/2.8 94o FOV
    - Remote having details DJI Model: GL300C
7. Identified Ports:
    - Micro USB

Identification of data storage locations:

- Relevant data storage locations in a UAV include removable memory cards (SD, Micro SD, etc.), fixed memory cards, flash memory (NAND, NOR, etc.). In the exhibit (DJI phantom 4) have a visible slot, which is designed to allow easy access and swapping of portable storage devices (memory card) and the same is the default storage location for media. An external memory card of 16 GB Panasonic SD card was found.

V. Methodology

a. Data Acquisition and preservation

1. *SD Card Imaging*: The external SD card of 16 GB used by the camera DJI, F/2.8 94o FOV was being used to store images and videos. We extracted the SD card from the drone and inserted it into a Cellebrite write blocked card reader. The SD card was imaged using the tool FTK imager. The SHA1 and MD5 hash were generated and stored.

2. *Drone Storage:* A separate memory card was found fixed to the motherboard. Flight log data is often stored in a single location. However, media files are often found in multiple locations, usually in different resolutions. The exhibit drone was examined and analyzed to retrieve the data/information using the forensic tool XRY. The data was successfully extracted; however, flight logs so found were being showed as 'unreadable' .kmz and. DAT files.

b. Data Analysis & Interpretation:

1. *SD Card examination:* The image of the SD card was further examined using software EnCase ver. 8.1. The .JPEG and .mp4 files recorded by the drone throughout the flight (Areal View) were extracted. The Micro SD card was then placed back into the case exhibit.
2. *Drone examination:* There were two primary sources for flight data from the DJI Phantom 4 that were extracted using XRY. The .DAT and .kmz files created by the drone were located on the drone's non-volatile internal storage.

i) DAT files: The final .DAT files were extracted and viewed using DatCon successfully. All relevant data were extracted. Unreadable .DAT files contained dates, sizes, etc; but no other legible data (see Table 1)

ii) .kmz files: These files were analyzed by using the tool Google Earth Pro [https://www.google.co.uk/earth/versions/#download-pro]. This mapping tool can be used for viewing flight data extracted from drones. Many co-ordinates at different positions and paths of the Drone flight (see Table 2).

VI. Result and discussion

The drone was fitted with a GPS tracking system and programmed to be able to autonomously fly from one location to another using GPS coordinates. Forensic data like images/videos and geolocations were analyzed using the forensic hardware/software tools and the results so obtained are tabulated in Table 1 and Table 2. In the present study, the data of DJI phantom 4 has been extracted, in which images/videos and GPS data was found, which will be helpful for investigating agencies to find out the locations of the drone used for malicious activities.

During the work on the drone DJI phantom 4 several .DAT files were found on the internal storage of the drone. These files followed a common naming convention of FLY***.DAT, where the "***" is a successive number. These type of files contain a large chunk of flight data related to the drone's location, flight status, and various sensors readings. The open-source tool Datcon converts these files to a readable .csv file format. However, this tool could not convert all of the data.

Name	File Ext	Logical Size	File Created
FLY044.DAT	DAT	86.75 MB	12/30/2017 10:06:28 AM (Device)
FLY045.DAT	DAT	257.09 MB	12/30/2017 11:33:10 AM (Device)
FLY046.DAT	DAT	126.38 MB	12/30/2017 3:38:56 PM (Device)
FLY047.DAT	DAT	148.94 MB	12/31/2017 8:14:08 PM (Device)
FLY049.DAT	DAT	7.66 MB	1/1/2018 3:42:24 PM (Device)
FLY050.DAT	DAT	220.59 MB	1/22/2018 11:32:48 AM (Device)
FLY051.DAT	DAT	38.88 MB	1/22/2018 11:33:50 AM (Device)
FLY052.DAT	DAT	165.06 MB	1/22/2018 1:36:58 PM (Device)
FLY053.DAT	DAT	348.56 MB	1/22/2018 1:40:44 PM (Device)
FLY055.DAT	DAT	203.34 MB	1/23/2018 11:16:54 AM (Device)
FLY057.DAT	DATS	68.78 MB	1/30/2018 4:21:10 PM (Device)

Table 1 .DAT and .kmz files and their properties

Sr. No.	DATE	TIME (UTC+05:30)	LATITUDE	LONGITUDE
01	12.30.2017	06:03:07 AM	25°26'15.64"N	93°56'14.64"E
02	01.22.2018	06:02:29 AM	25°10'49.23"N	94°15'48.68"E
03	01.22.2018	06.03.47 AM	25°26'24.45"N	93°55'02.67"E
04	01.23.2018	05.51.37 AM	25°10'05.50"N	94°17'23.80"E
05	11.24.2017	06:36:37 AM	25°41'58.15"N	93°34'20.31"E
06	05.03.2019	11:12:21 AM	25°51'29.50"N	93°45'44.98"E
07	01.01.2018	10:12:11 AM	28°04'29.64"N	92°24'50.10"E
08	01.30.2018	10.51.10 AM	35°23'06.33"N	47°42'27.87"N
09	05.03.2019	10:59:45 AM	25°51'29.53"N	93°45'44.93"E
10	02.11.2020	09:53:57 AM	60°45'33.27"N	157°42'31.39"E

Table 2 Co-ordinates at different positions and path of the Drone flight

The .kmz files retrieved using XRY were further analyzed by Google Earth Pro [https://www.google.co.uk/earth/versions/#download-

pro]. This mapping tool was used for viewing flight data extracted from logs. The retrieved geolocations, launch point, and flight path (see Figure 3, Figure 4. and Figure 5.). Both files were encrypted and encoded using two different formats. These files contain the data regarding the GPS, motors, remote control, flight status, and other information.

Figure 3 - Recovered Geolocations

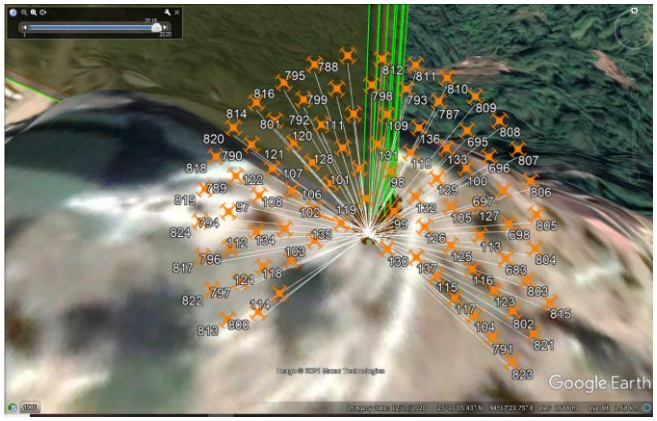

Figure 4 - Recovered Geolocations

Figure 5 - Recovered Geolocations

VII. CONCLUSION

In the present case study, we examined and evaluated DJI Phantom 4 (Drone) through well-known digital forensic tools. We discussed the data and geo-locations to interpret the recovered flight data from DJI Phantom 4(UAV). The .DAT and .kmz files were retrieved from the drone's internal memory, which contained a large number of flight data. The data present in the SD card i.e.; more than 200 aerial images and 30 video files, which were captured and stored during the flight, were retrieved. The findings of this case study reveal that all captured images (.JPEG) including videos (.mp4) as well as the drone flight movement details i.e. GPS/location could be successfully traced. At the end of the investigation, information about the whole flight was acquired; GPS detail of each flight path, camera images & videos, creation date and time of images, image positions, were successfully retrieved.

VIII. Acknowledgement

The authors gratefully acknowledge the support given by Dr. S K Jain, Director cum-CFS, DFSS, MHA, GOI, New Delhi.

IX. REFERENCES

[1]. David Kovar. (2015). UAV (aka drone) Forensics. Available: https://files.sans.org/summit/Digital_Forensics_and_Incident_Response_Summit_2015/PDFs/ForensicAnalysisofsUASakaDronesDavidKovar.pdf. Last accessed 18 March 2018.

[2]. Gonzalo De La Torre, Paul Rad and Kim-Kwang Raymond Choo. (2018). Driverless vehicle security: Challenges and future research opportunities. Future Generation Computer Systems. DOI: https://doi.org/10.1016/j.future.2017.12.041.

[3]. Devon R.Clark, Christopher Meffert, Ibrahim Baggili and Frank Breitinger. (2017). DROP (Drone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. Digital Investigation. 22(Supplement): S3-S14.

[4]. M. Faheem, Kechadi, M-T., N-A. Le-Khac, 'The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trend'. International Journal of Digital Crime and Forensics, 7 (2):1-19, 2015

[5]. R. Witteman, A. Meijer, N-A. Le-Khac, M-T. Kechadi (2016), "Toward a new tool to extract the Evidence from a Memory Card of Mobile phones", 4th IEEE International Symposium on Digital Forensics and Security, Arkansas, USA, April 2016

[6]. Da-Yu Kaoa, Min-Ching Chena, Wen-Ying Wua, Jsen-Shung Lina, Chien-Hung Chenb, Fuching Tsaic,* (2019),

[7]. A. Roder, K.-K. R. Choo, N.-A. Le-Khac, Unmanned Aerial Vehicle Forensic Investigation Process: Dji Phantom 3 Drone as a Case Study, arXiv preprint arXiv: 1804.08649.

[8]. Horsman, G., 2016. Unmanned aerial vehicles: a preliminary analysis of forensic challenges. Digit. Invest. 16, 1-11.

[9]. Jain, U., Rogers, M., Matson, E.T., 2017. Drone forensic framework: sensor and data identification and verification. In: Sensors Applications Symposium (SAS). IEEE, pp. 1-6. IEEE, 2017

[10]. Prastya, S.E., Riadi, I., Luthfi, A., 2017. Forensic analysis of unmanned aerial vehicle to obtain gps log data as digital evidence. Int. J. Comput. Sci. Inf. Secur. 15 (3), 280

[11]. F. I. H Bouafif, F Kamoun, A. Marrington, Drone Forensics: Challenges and New Insights, 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)doi:10.1109/NTMS.2018.8328747

[12]. S, A., P, A., C, A., Mhatre, V., Chavan, S., Kumar, N., 2015. Embedded video processing and data acquisition for unmanned aerial vehicle. International Conference on Computers, Communications, and Systems. https://doi.org/10.1109/ CCOMS.2015.7562889

Cite this article as :

A. Pathania, D. P. Gangwar, Shivanshu, Poonam, Arpita Angrish "Unmanned Aerial Vehicle Forensic Investigation Process : Dji Phantom 4 Drone as A Case Study", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 4, pp. 593-599, July-August 2021. Available at
doi : https://doi.org/10.32628/CSEIT2174136
Journal URL : https://ijsrcseit.com/CSEIT2174136