Chapter 10
UAV Forensics: DJI Mavic Air Noninvasive Data Extraction and Analysis

Siniša Husnjak, Ivan Forenbacher, Dragan Peraković, and Ivan Cvitić

10.1 Introduction

Unmanned aerial vehicles (UAVs), also referred to as drones in the literature, can be defined as an aircraft piloted by remote control or an onboard computer. UAVs can be considered as a part of the broader unmanned aerial system (UAS), which encompasses UAV, ground control station (GCS), controller, and associated applications [1].

The UAS technology is a rapidly emerging technology and it has found widespread usage. According to the report available at [2], the global UAV market will grow from $14 billion in 2018 to over $43 billion in 2024 at a CAGR of 20.5%. Considering the increasingly popular use of UAVs, it is evident that there is potential for them to be used in crimes. Also, criminal UAV operations are increasing rapidly and criminals are constantly developing new approaches. This demands a forensics investigation. UAV forensics is valuable for many types of UAVs investigations, including:

- Commercial aerial surveillance
- Disruption of airports and air traffic activities
- Smuggling of drugs, smartphones, knives, or guns—often into prisons
- Oil/gas/mineral exploration and disaster relief
- Delivery of improvised explosive device into public places by terrorists using UAVs
- Invasion of privacy by press or paparazzi
- Espionage of security and intelligence agents

S. Husnjak · I. Forenbacher · D. Peraković (✉) · I. Cvitić
Faculty of Transport and Traffic Sciences, University of Zagreb, Zagreb, Croatia
e-mail: shusnjak@fpz.unizg.hr

L. Knapčiková et al. (eds.), *5th EAI International Conference on Management of Manufacturing Systems*, EAI/Springer Innovations in Communication and Computing, https://doi.org/10.1007/978-3-030-67241-6_10

The camera mounted onto a drone, either as a static recording or a live streaming device, raises significant data privacy concerns for organizations and the public. Also, the ability of drones capturing pictures or videos of operations in designated no-fly-zone areas of airspace, such as airports, military base, and power stations, presents a significant security threat [3]. This urges the research community to develop techniques to detect and prevent illegal activities which involve UAVs.

UAV is an example of a widely used technology that requires the collection of a solid body of evidence to help eliminate potential real-world threats [4, 5]. Despite its increased importance, UAV forensics is still a relatively unexplored research topic. Commercial tools (e.g., Cellebrite, Oxygen Forensic, MSAB) are in their early stages when it comes to UAV forensics. This is because of the different types of drones which require a log parser and visualizer, which support all types of available software [4].

This research paper presents the acquisition and analysis of important digital artifacts found on both the internal memory of the UAV and the controlling application. Forensic analysis of flight logs, media files, and other important files of UAV and controlling application for identifying digital artifacts was done by a commercial forensic tool that meets all the guidelines on the admissibility of evidence.

10.2 Previous Research: Literature Overview

UAV/UAS forensics is a relatively new and less studied domain, in comparison to other popular consumer devices and technologies, such as computers and mobile devices. Only a few research papers performed some type of UAV, UAS, or drone forensics.

Research [6] presents an introductory discussion of UAV analysis and provides the results of a digital forensic investigation of a Parrot Bebop UAV. Further, research [7] performed a forensic investigation of an UAS—the DJI Phantom 2 Vision Plus. Research [8] thoroughly conducted a forensic analysis of the DJI Phantom 3 drone and the primary account for proprietary file structures stored by the examined drone. It also presented forensically sound open-source tool DRone Open source Parser (DROP) that parses proprietary DAT files extracted from the UAV's nonvolatile internal storage.

Authors in [3], presented the extraction and identification of important artifacts from the recorded flight data as well as the associated mobile devices using open-source tools and some basic scripts developed to aid the analysis of two popular drone systems: the DJI Phantom 3 Professional and Parrot AR. Drone 2.0. Further, research [9] presented a forensic analysis of UAV to obtain GPS log data as digital evidence.

In research [10], a forensic investigation on an UAS was performed, specifically the DJI Mavic Air, using an iOS-based smartphone device. This study examined the data that can be extracted from the UAS in addition to investigating and analyzing

the logical acquisition of the associated smartphone device created by Apple's iTunes backup utility. Research [4] examined digital evidence and artifacts using the benchmark drone forensic images of the Yuneec, Inc. Typhoon H UAV, and authors in [11] examined and analyzed the data extracted from four DJI drone models.

Most of the mentioned research papers focused on digital forensic investigation involving free and/or open-source software for data acquisition, analysis, and reporting. Further, regarding data parsing and encryption, most of them used open-source tools.

As many research papers, the investigation presented in this paper is focused on the investigation of available DJI UAV, but the main difference regarding other studies involves the usage of commercial forensics tools regarding all of the investigation phases—acquisition, decryption, parsing, analysis, and reporting—thus providing forensically sound and acceptable investigation.

10.3 Sources of Data/Information/Evidence

UAVs are a potential source of evidence in a digital investigation, partly due to their increasing popularity in our society [1]. The artifacts that may be contained by a UAV could be analyzed in two groups such as physical and digital evidence. Physical evidence contains UAV, flight controllers, sensors related with drones, ground control stations, mobile devices and applications, etc. Digital evidence is located on the physical devices and their storage and communications links: the UAVs, batteries, sensors, remote controller, the GCS station, and on any devices used to control the UAV or process its data. In this research paper, the focus is on digital evidence.

After capturing the UAV, 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 navigation, as well as the camera and digital storage [3, 12].

The sample UAS which was used in this research is DJI Mavic Air, which consists of two main components: the UAV and the GCS; it has four propellers, a stabilized gimbal and a 4K resolution camera, GPS antennas, a MicroSD card slot, and a USB-C port. The aircraft also has 8 GB of internal storage. The GCS consists of the remote controller and the mobile device that is used to run the DJI GO 4 application. The Mavic Air utilizes a Wi-Fi transmission system and can fly for 21 min with a maximum flight distance of 10 km [10]. UAS contains not only the UAV but also the whole system which is used for airworthiness such as GSCs, mobile devices, connected applications, cloud services, communication links, etc.

UAVs will routinely create and store usage logs that can include details such as mission details, time and date of operations, and navigational waypoints during use. This data will generally consist of GPS positions, motor speeds, altitude, and directional information [13]. UASs contain four general types of data that could be presented as evidence, explained further in Sects. 10.3.1–10.3.4.

10.3.1 DAT File(s)

First one of the artifacts that sample UAS (DJI Mavic Air) contained was a DAT extended binary file. This file is located on the nonvolatile internal memory of the UAV (8 GB capacity regarding DJI Mavic Air). It was found in [14] that the UAV creates a new DAT extended file on every startup.

Regarding DJI Mavic Air, these DAT files extracted from UAV are encrypted and encoded, but DAT files extracted from a DJI GO 4 application were not encrypted. The structure of a DAT flight record files, generally speaking (when DAT files are not encrypted and encoded), is presented in Fig. 10.1.

Analysis of these data can reveal the actions of the drone during flight. For example, GPS coordinate can reveal from where the drone took off, or in the event of a crash, battery levels can reveal the time when the drone failed as it can be correlated with time. These data can also be used to reconstruct the flight, which is especially important when the drone has been used in smuggling or other flight-related crime [3].

UAS data, when correctly extracted and accurately analyzed, provide valuable intelligence about launch locations, flight profiles, and logistical and operational linkages, and data packet types which can be found in DAT file are presented in Table 10.1.

The UAV should not be turned on as turning it on changes data on the UAV by creating a new DAT file, but may also delete stored data if the drone's internal storage is full [8].

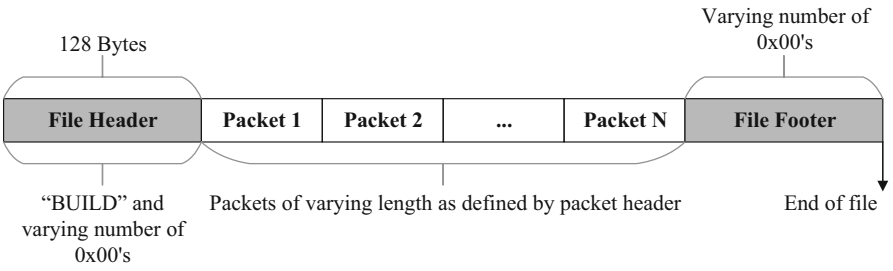

Fig. 10.1 General structure of DAT extended flight record files [8, 14]

Table 10.1 DAT extended flight record file packet type values [14]

Packet type	Value	Packet type	Value
GPS	0xCF01	Home point	0xC60D
Motor	0xDAF1	Tablet location	0xc12B
Gimbal	0x2C34	Remote control	0x9800
Flight status	0x2A0c	Battery	0x1E12
Advanced battery	0x4411		

Table 10.2 TXT extended flight record file packet type values [14]

Packet type	Value	Packet type	Value
On-screen display (OSD)	0x01	Advanced battery	0x08
Home point	0x02	Application messages	0x09
Gimbal	0x03	Application warnings	0x0A
Remote controller	0x04	Remote controller GPS	0x0B
Time	0x05	Aircraft GPS	0x0E
Battery	0x07	Firmware	0x0F

10.3.2 TXT File(s)

Flight logs TXT type of data was stored on the mobile device which runs "DJI GO 4" application. This file is a binary file, has TXT extension, and contains a very detailed flight record. According to [15], the flight logs of TXT files record GPS coordinates, timestamp, motor speed, and other data which are stored in the internal storage of the UAV. General packet type values of a flight record TXT file are shown in Table 10.2.

Authors in [3] emphasize that de-compilation of the DJI GO application revealed the Service Set Identifier (SSID) and password required to gain access to network for the DJI Phantom 3 Professional. According to [14], the TXT file footer contains some specific information about the UAV in plaintext; like flight area and a screenshot of a home point, name and model of the UAV and serial numbers of inertial measurement unit (IMU), camera, mainboard of the remote control, and battery.

Through a flight control system, Wi-Fi information of a drone can be set or modified. The flight data files stored in the drone's internal SD card storage can be downloaded [15].

10.3.3 EXIF File(s)

According to [13], in most cases, the primary and largest source of data stored by either recreational or commercial UAVs will consist of digital imagery or video footage. Photos and videos taken by the drone in flight mode are stored in SD card [15]. Also, our research found that, regarding tested UAV, mentioned storage includes both internal and/or external storage (SD card), depending on the UAV settings.

According to [16], two of the artifacts are log files stored as binary files and the other artifact is the Exchangeable Image File Format (EXIF) header of the images that are captured by the UAV's onboard camera.

EXIF header of the images, which is taken by UAV's onboard camera, contains lots of valuable information, in terms of investigation. There are also lots of tools

which can extract the EXIF metadata from the images like location, altitude, creation time and modification times, information about the camera and settings, etc.

10.3.4 Identification, Sensor, and Log File(s)

UASs contain not only DAT and TXT flight information and EXIF files but also other types of files which include valuable information as a digital footprint of the device, user, activity, and involved subjects of the investigation.

These files could include extensions like LOG—which mostly include some log files of application, device, and user's activities; CONF—which generally provides information about configurations and settings; or TXT—which doesn't include extended flight information but involves other information like IDs of the devices, cameras and their sub-elements, firmware versions of software, factory data information, etc.

10.4 Methodology

Detailed methodology of the UAS is described in [1], with set of guidelines for UAS investigations. The study reported in this paper focused on data which could be extracted from different elements of UAS. Regarding that, in this research paper, a general forensic investigation methodology of an UAS was used, which also incorporated principles and elements of proposed guideline to ensure the integrity of the original data. Five-step investigation methodology is presented in Fig. 10.2.

According to [14], in order to investigate a UAV forensically, its hardware and software components should be identified. Besides the investigation of the UAV components, collecting evidence, providing a chain of custody, and media/artifact analysis are important parts of the forensic investigation. Table 10.3 shows the list of hardware and software used in this research.

As a first step, factory reset procedures were performed for the UAV and connected mobile device (Samsung SM-G955F) before performing planned flights. The UAVs storage was formatted by using DJI GO 4 application. This process removes all nonvolatile files that are stored on the internal memory of the drone. Android mobile device was formatted to factory settings by using booting menu.

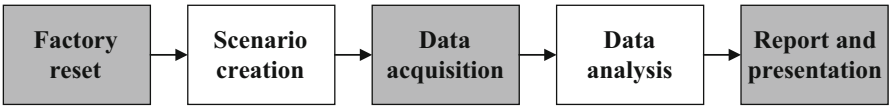

Fig. 10.2 Five-step investigation methodology used in research

Table 10.3 Hardware and software tools used for the research

Tool	Description	Utilization
Flight system		
DJI Mavic Air	Quadcopter/Model: U11X	Flight scenario simulation
DJI remote controller	Remote controller/Model: S01A	Flight control
Samsung SM-G955F	Android OS/v9.0.0.	UAV control and navigation
DJI GO 4	Heads up display/v4.3.36	Navigation/live video feed
DJI Assistant 2	Software support/v1.2.5	SW update/data verification
Forensic analysis tools		
Forensic workstation	Windows 10 Pro 64-bit	Forensic tools execution
CsvView	Version 3.7.5	TXT data files parsing
UFED Touch 2	Version 7.32.0.68	Data acquisition
Physical analyzer	Version 7.32.0.16	Data analysis and presentation

After the formatting, mobile device was updated to the latest Android version and the latest version of DJI GO 4 application was installed. UAV was updated by using DJI Assistant 2 software, connected to the forensic workstation. SD card located in the UAV was formatted to FAT32 file system.

The second step included scenario creation which incorporated simulation of typical UAS activities like flights in different areas and times, picture footage and video recording, home-point activation, settings adjustment, etc. This research focused on the forensic analysis of a simulation of a captured UAV and a mobile device as a GCS.

Data acquisition phase included a collection of all possible data based on approved forensically sound techniques. In fourth, data analysis phase, the authors investigated data acquired from the UAS and tried to find all relevant evidence about possible cases. The report and presentation phase was a final step of the digital forensics investigation process, partly given by this research paper.

10.5 Data Acquisition

UASs are still in their development phase without any existing commonly accepted standards for their underlying technologies and their forensic investigation [16]. Traditional forensic tools may successfully extract media files; however, flight logs may show as “unreadable.” UAS manufacturers may store data in different formats and currently, there is no standardization. Should any data be identified, consideration must be given to checking the data through another tool and confirming that it has been interpreted correctly [1].

Typical digital forensic analysis is normally conducted using commercial forensic tools, which will usually have a proven record for accuracy. Any examination using non-validated tools is considered a risk. However, until commercial forensic tools for all UASs are available, we may have little choice but to rely on open-source

Table 10.4 UASs elements and their description

No.	UAS acquisition part	Description/example
1.	UAV internal storage	Aircraft—main element of an UAV
2.	UAV external storage	SanDisk SD card
3.	Mobile/tablet device	Flight control connected to remote controller
4.	Mobile application	Flight control application installed on mobile device
5.	Remote controller	DJI flight remote controller
6.	Cloud service	Data storage and account for the cloud service
7.	Assistant application	Application for software/firmware update and log files
8.	Mobile/tablet device backup	Backup of a flight control device
9.	First person view goggles	Additional device for flight control options
10.	Network packet data	Communication through wireless networks
11.	SIM card	UAVs embedded or traditional SIM card

tools to extract data of forensic interest. As previously discussed, the capabilities of such open-source tools can vary significantly. In some cases, extracted data can provide significant information, while others may only provide limited data. Examples of such tools include DatCon, DJIFix, st2dash, and DroneLogbook [1].

This research considered data extraction of data sources that do not require invasive or destructive methods (e.g., JTAG, ISP-eMMC, Chip-off). Destructive methods make a risk in future usage of UAS and should only be considered when all other methods fail.

Table 10.4 provides the most comprehensive analysis of the possible elements of a typical UAS and thus possibilities for data storage, transmission, and afterward data acquisition regarding forensics investigations.

Multiple systems are involved in providing the full functionality of DJI Mavic Air UAS and thus, in this research, data acquisition was conducted on UAV and smartphone application DJI GO 4 (parts 1–4 from Table 10.1), as parts of this UAS and primary goal of this research. Commercial forensic tools (UFED Touch 2 and Physical Analyzer) from Cellebrite, Inc. were used to perform data acquisition, analysis, and reporting, providing very unique opportunities regarding the forensic analysis of DJI Mavic Air UAS, involving noninvasive and nondestructive data acquisition as important goals of this research.

UASs elements seen in Table 10.4 and numbered from 5 to 11 are not part of this research paper. Also, our research wanted to emphasize that there are also other UASs elements which could contain valuable investigation data—and this is planned to be analyzed in some future research.

10.5.1 UAV's Data Acquisition

Linux is the predominant OS for onboard UAV systems and it is possible to perform mobile forensic techniques to collect the data from the drone [3].

UAVs data acquisition in this research included:

1. internal (onboarded) and
2. external

storage data extraction, by using mentioned commercial forensic tools and providing noninvasive extraction methods. Extraction methods used in this research regarding UAV device (internal and external storage) were file system and physical extraction. Both extractions were performed by connecting UAV (by USB cable) with the UFED Touch 2 used for data extraction.

UAV's internal mounted storage was a micro SD card (8 GB storage) permanently attached to the main board of the UAV. Extracted files included TXT, LOG, and DAT extension of files which provide information about: ID of the UAV's elements, system log files, encrypted flight logs, Wi-Fi and factory configuration settings, etc.

UAV's external storage was a SanDisk micro SD card (128 GB storage). Recorded media files are stored on a FAT-formatted external micro SD card. Formats used for media are JPEG for images and MP4 for video files. The file names consist of a "DJI" prefix followed by an *n*-digit serial number which increments each time a new file is created (e.g., DJI_0007.JPG).

10.5.2 Mobile Device and DJI GO 4 Data Acquisition

The GCS consists of a remote controller and the mobile device that is used to run the DJI GO 4 application. This application provides real-time image transmission and camera settings adjustments and creates a detailed flight record that is stored on the mobile device. Mobile device Samsung SM-G955F was used for running DJI GO 4 application.

File system mobile forensic extraction method was performed by connecting mobile device (by USB cable) with the UFED Touch 2 used for data extraction. This extraction provided files and potential evidence which can be found on a mobile device with installed DJI GO 4 application.

Both extractions (UAVs and DJI GO 4s) provided many important digital evidence which could benefit potential forensic investigation. Results were analyzed by Physical Analyzer and can be seen in discussion of this research paper.

10.6 Discussion: Data Analysis and Presentation

There are various types of data which assist the investigation of UAS incidents. Data analysis phase included analysis of acquired data from acquisition phase—UAV internal and external storage and mobile device application DJI GO 4 acquired data. Analysis of data was made by commercial forensic software Physical Analyzer and CsvView.

Since data analysis phase provides a lot of valuable information regarding potential digital evidence, it is hard to exclude the most important artifacts. Those files and their value are associated with exact investigation, but the potential of all acquired data is enormous since it gathers other valuable data of a user's activities and devices. Table 10.5 provides anonymous information about potential evidence gathered into categories and provides some details regarding some of the data.

According to data provided by Table 10.5, forensic analysis could provide a lot of useful information regarding the digital investigation.

Table 10.5 Types and examples of recoverable data by UAV and DJI GO 4 acquisition

Data type	Found/extracted	Examples/utilization
Identification	Drone serial number	0K1CGCER######
	Batteries serial number	0K4AH14A######
	Board ID	0K5CGCA0######
	Device ID	0K1CGCER######
	User account(s)	name.surname@gmail.com
	Factory data	Year: 20 month: # Day: 14
Multimedia content	Images—UAV	DJI_####.jpg
	Videos—UAV	DJI_####.MP4
	Images—DJI GO 4	DJIFlightRecord_2020-##-##.jpg
	Videos—DJI GO 4	2020_04_26_18_10_56.mp4
Multimedia activity	Panorama.log	Time: 2020-4-26_18:19:18
	DJI Go 4 DAT	Flight record details
	DJI Go 4 TXT	Flight record details
	Timestamp_check_log	####video start, Sun Apr 26
	Video_drop_frame_log	****video stop, total drop 0 frames
Wi-Fi connection	SSID	ssid=MAVIC_AIR####
	Passphrase	a157####
	Hostapd.conf	channel=7
Flight logs	Longitude	46.226708
	Latitude	16.120406
	Elevation	208,263000488281
	Timestamps	26.4.2020. 16:24:23
Metadata	Camera make	DJI
	Camera model	FC2103
	Capture time	26.4.2020. 18:23:58
	Pixel resolution	4056 × 3040
	Resolution	72 × 72 in.
	Lat/Lon	46.226710/16.120405
Automated usage logs	Power off battery	[L-CMD] power off
	UAV motor log	[L-FMU/MOTOR] read motor
	Takeoff	[L-TAKEOFF] alti: 210.981033
	Battery warning	[L-FMU/LED] battery warning!

Identification of data files provides information regarding devices, their internal components, and users' identities like serial numbers, accounts IDs, etc. Some identification files were encrypted, like UAVs firmware version.

Multimedia content presents information about images and video files and their content, extracted from UAV and DJI GO 4. Depending on the data extraction method, deleted files from unallocated space can also be recovered and analyzed.

Multimedia activity data provided information about details of activities which are involved in creating multimedia content. Those data provide geolocation information for critical locations—launching, landing, and home or return locations; also provided full flight path information and timestamps of involved activities. DAT files extracted from UAV were encrypted and encoded, as mentioned in the previous text. DAT and TXT files available from extraction of a DJI GO 4 application were not encrypted. Research [8] also shares findings on TXT files, which are proprietary, encrypted, encoded on UAV, and also found on the mobile device controlling the drone. These files provided a slew of data such as GPS locations, battery, flight time, etc. Findings indicate that the DJI GO 4 application used to control the UAV contains a significant amount of unencrypted forensic data.

Wi-Fi data like SSID and password were found. Flight logs are very important part of UAS forensics and they were extracted from DAT and TXT files.

Metadata of images and video are available in detail, just like automated usage log files (UAV telematics, diagnostic error codes, power on and shutdown times, system events, etc.) made by UAV itself and correlated with timestamps.

The last phase of the five-step investigation methodology used in research includes reporting and presentation of results. This phase is partially made through this research paper and provided results of data acquisition and analysis, and all other data are available upon request. In UAV forensics, a lot of interest involves flight logs. Figure 10.3 provides visualization of flight records and UAV's journey's, gathered from acquired data, analyzed, visualized, and validated by using two forensic tools.

As mentioned before, DAT and TXT extended flight records extracted from DJI GO 4 application, provided detailed information about UAV's journeys. Those journeys can be seen in Fig. 10.3, which provides a comparative analysis of the results of visualization of two forensic tools.

Fig. 10.3 Visualization and presentation of UAV flight log files; Physical Analyzer (left) and CsvView (right)

Both visualizations are made from one DAT file extracted from DJI GO 4 application. Picture on the left from Fig. 10.3 provided visual information available after analysis by forensic tool Physical Analyzer and his parsing capabilities, while the picture on the right provided visual information available after analysis by tool CsvView. According to [3], there are many online services offering interpretation of DAT files, however, uploading evidence to a third-party server is not appropriate for a forensic investigation or intelligence purposes, so there was a tool designed to interpret and visualize these files—CsvView, used also in this research.

After analyzing similarities and differences, there are minor differences regarding visualization points and flight logs. This also provided cross-verification of forensic tools and thus providing the admissibility of evidence.

10.7 Conclusion

UAVs will have an increasingly more important role in the future of digital forensic investigations. Those devices are becoming more sophisticated and their usage becomes more needed—from legitimate to non-legitimate activities. As a valuable source of potential digital evidence, the use of UAVs could greatly enhance the efficacy of a digital investigation.

Digital forensic analysis of UAVs is increasingly used to determine if a device has been used for a non-legitimate activity. Due to the recent societal use of UAV devices and their services, the need for UAV forensics will become a necessity.

The proposed work in this research presents forensic investigation on a DJI Mavic Air UAV and associated smartphone app DJI GO 4 installed on the Android device. The proposed methodology used five-step investigation process, which included the use of commercial forensic tools that do not require invasive or destructive methods for data acquisition and analysis.

By analyzing acquired data, authors located information about the possible sources of evidence grouped into few categories depending on the type of the acquired data. Also, details about possible digital evidences have been provided. This research also provided a comprehensive overview of elements of a typical UAS and provided a forensic analysis of the most important elements of an UAS.

The outcome of this research study can be seen in a few ways: investigation of possible elements of an UAS for the purpose of forensic analysis, examples of data which are available for the use of a specific UAV (DJI Mavic Air), and possibilities of commercial forensic tools for the purpose of acquisition, analysis, parsing, and visualization of gathered data.

Further research of this should investigate other sources of UAS forensics such as cloud services and remote controller possibilities for the purpose of forensic analysis. Also, there is a need to make a comparative analysis of other commercial and open-source digital forensics software in order to enhance investigation efficiency, verify forensic software, and provide more valuable digital evidence.

Acknowledgments The network "DigForASP—Digital forensics: evidence analysis via intelligent systems and practices" is funded by the European Cooperation in Science and Technology (COST) under the Horizon 2020 framework program.

References

1. A. Roder, K.K.R. Choo, N. Le-Khac, Unmanned aerial vehicle forensic investigation process: DJI phantom 3 drone as a case study, Cryptography and Security, 2018, pp. 1–14. arXiv:1804.08649
2. Droneii, The drone market report 2019–2024, https://www.droneii.com/project/drone-market-report. Last accessed 28 Apr 2020
3. M.A. Hannan, B. Azhar, T. Edward, A. Barton, T. Islam, Drone forensic analysis using open source tools. J. Digit. Forensic Secur. Law **13**(1), 23–35 (2018)
4. F.E. Salamh, U. Karabiyik, M.K. Rogers, RPAS forensic validation analysis towards a technical investigation process: A case study of Yuneec Typhoon H. Sensors **19**(1), 36–49 (2019)
5. D.A. Hamdi, F. Iqbal, S. Alam, A. Kazim, A. MacDermott, Drone forensics: A case study on DJI phantom 4, in *IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, (IEEE, Abu Dhabi, 2019), pp. 17–23
6. G. Horsman, Unmanned aerial vehicles: A preliminary analysis of forensic challenges. Digit. Investig. **16**, 1–11 (2016)
7. M. Maarse, L. Sangers, *Digital Forensics on a DJI Phantom 2 Vision+ UAV* (University of Amsterdam, Amsterdam, 2016)
8. D.R. Clark, C. Meffert, I. Baggili, F. Breitinger, DROP (DRone open source parser) your drone: Forensic analysis of the DJI phantom III. Digit. Investig. **22**, S3–S14 (2017)
9. S.E. Prastya, I. Riadi, A. Luthfi, Forensic analysis of unmanned aerial vehicle to obtain GPS log data as digital evidence. Int. J. Comput. Sci. Inf. Security **15**, 280–285 (2017)
10. M. Yousef, F. Iqbal, Drone forensics: A case study on a DJI Mavic Air, in *IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, (IEEE, Abu Dhabi, 2019), pp. 1–3
11. M. Yousef, F. Iqbal, M. Hussain, Drone forensics: A detailed analysis of emerging DJI models, in *11th International Conference on Information and Communication Systems (ICICS)*, (IEEE, Irbid, 2020), pp. 66–71
12. F. Iqbal et al., Drone forensics: Examination and analysis. Int. J. Electr. Secur. Digit. Forensics **11**(3), 245–264 (2019)
13. Interpol, *Framework to Responding to a Drone Incident* (Digital Forensics Laboratory of the Interpol Innovation Centre, Singapore, 2020)
14. I. Gulatas, *Unmanned Aerial Vehicle Digital Forensic Investigation* (The Republic of Turkey Bahcesehir University, Istanbul, 2018)
15. D.Y. Kao et al., Drone forensic investigation: DJI spark drone as a case study. Proc. Comput. Sci. **159**, 1890–1899 (2019)
16. S. Baktir, İ. Gulatas, Unmanned aerial vehicle digital forensic investigation framework. J. Naval Sci. Eng. **14**(1), 32–53 (2018)