Journal of Naval Sciences and Engineering
2018, Vol. 14, No.1, pp.32-53
Computer Engineering/Bilgisayar Mühendisliği

RESEARCH ARTICLE

UNMANNED AERIAL VEHICLE DIGITAL FORENSIC INVESTIGATION FRAMEWORK

İbrahim GÜLATAŞ[1]
Selçuk BAKTIR [2]

[1]Computer Engineering, Bahcesehir University, Besiktas, Istanbul, Turkey, igulatas@hotmail.com
[2]Computer Engineering, Bahcesehir University, Besiktas, Istanbul, Turkey, selcuk.baktir@eng.bahcesehir.edu.tr

Date of Receive: 04.03.2018 **Date of Acceptance: 03.04.2018**

ABSTRACT

The Unmanned Aerial Vehicle (UAV) technology is a rapidly emerging technology and it has found widespread usage. While UAVs are still in their development phase without any existing commonly accepted standards for their underlying technologies and their forensic investigation, they have an increasing record of criminal usage. This urges the research community to develop techniques to detect and prevent illegal usage of UAVs. With this work, we present a seven-phase UAV digital forensics investigation framework to standardize the investigation process for UAVs. We tested our framework on the DJI Phantom III Professional UAV which is one of the most popular commercial UAVs in the market. Three kinds of forensic artifacts are found on the sample UAV and these artifacts are examined deeply. Two of the artifacts are log files stored as binary files and the other artifact is the EXIF header of the images that are captured by UAV's onboard camera. As a result of our investigation, we are able to regenerate the flight path of the UAV. As a final step of our research, we compare our investigation framework with the existing framework on the literature and reveal the differences of both frameworks.

Keywords: *Digital Forensics Investigation, Embedded Devices Forensics, Unmanned Aerial Vehicle (UAV) Forensics.*

İNSANSIZ HAVA ARAÇLARI İÇİN ADLİ BİLİŞİM İNCELEMESİ ÇERÇEVESİ

ÖZ

İnsansız Hava Araçları teknolojisi günümüzün hızla gelişen teknolojileri arasında yer almaktadır. İnsansız hava araçlarının kullanımındaki hızlı artış, bu araçların yasadışı faaliyetlerde kullanımını da beraberinde getirmiştir. İnsansız hava araçlarının yasadışı kullanımlarının tespiti ve önlenmesi çözülmesi gereken önemli bir problem olarak ortaya çıkmıştır. Bu çalışmada insansız hava araçlarının adli bilişim incelemelerinde kullanılmak üzere yedi aşamalı bir inceleme sistemi ortaya önerilmektedir. Önerilen bu sistem şu an piyasada kullanılan en popüler ticari insansız hava araçlarından biri olan DJI Phantom III professional insansız hava aracı üzerinde uygulanmıştır. Yapılan incemeler sonucunda incelenen insansız hava aracında üç adet delil tespit edilmiştir. Bulunan bu delillerin iki adedi uçuş kayıt dosyası, diğeri ise araçta bulunan kamera tarafından çekilen görüntü dosyalarındaki metadata bilgileridir. Dosyalar üzerinde yapılan incelemeler sonucunda insansız hava aracının gerçekleştirdiği uçuşlara ait GPS koordinatları ve uçuş haritaları elde edilmiştir. Araştırmamızın son aşaması olarak ortaya önerdiğimiz inceleme sistemi şu anda literatürde bulunan diğer inceleme sistemi ile karşılaştırılarak farklılıklar belirtilmiştir.

Anahtar Kelimeler: *Adli Bilişim İncelemesi, Gömülü Sistemler Adli Bilişim İncelemesi, İnsansız Hava Araçları (İHA) Adli Bilişim İncelemesi.*

1. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) have become increasingly popular to use, with a wide range of usage areas throughout the world. While the first UAVs were used as early as on 22 August 1849 in Austria to launch the first air raids in history to the Venice [1], UAVs have found widespread usage only in recent years. It is reported that there are 770,000 hobbyists and 80,000 commercial Unmanned Aerial System (UAS) pilots had registered as UAS pilots in the United States as of 2017 [2, 3]. By 2021, it is expected that there will be around 3,5 million UAVs used by hobbyists [4].

Due to their significantly reduced prices, it has become easier to own and

fly a UAV, and some people have started using UAVs also for illegal purposes such as terrorism, plane watching, violation of private life, smuggling and delivery of drugs into prisons [5, 6]. Since the illegal usage UAVs, in violation of the Federal Aviation Administration (FAA) regulations [7], is increasing dramatically, it has become crucial to have the ability to detect and prevent illegal usage of UAVs. Furthermore, it is vital to have the ability to find and show evidence of illegal UAV usage when a case is brought in front of the court. The increasing number of illegal UAV usages has drawn closer public attention when a UAV crashed into a lawn at the White House [8, 9]. This incidence clearly reveals the necessity for standardized digital forensic investigation methods to obtain evidence for UAV related criminal incidences, so that they can be prosecuted in front of the court.

There is no standardized framework for digital forensics investigation of UAVs at the time of this study. With this work, we aim to fill this gap and propose a framework for the digital forensic investigation of UAVs. The proposed framework is applied on DJI Phantom III, one of the most popular commercial drones available in the market today. During the implementation of our framework, we kept in mind the well-known forensic investigation principles such as preserving digital evidence, preserving chain of custody, avoiding adding data and documenting actions [10].

In Section 2, we give a literature review on the digital forensic investigation of UAVs. In Section 3, we propose our UAV digital forensics investigation framework and apply this framework to the digital forensic investigation of the DJI Phantom III UAV. In Section 4, we implement the proposed framework on our sample UAS. In Section 5, we test and compare our framework with the other existing framework on the literature. Finally, in Section 6, we give our conclusions and propose future research directions.

2. RELATED WORK

A UAV is defined as a pilotless aircraft or a flying machine without an onboard flying pilot and passengers. In this definition, "unmanned" defines the complete absence of humans [11]. The related term UAS was first introduced by the U.S. Department of Defense (DoD), which was followed by FAA and European Aviation Safety Agency (EASA) [12]. According to

its definition, a UAS contains not only the aircraft but also the whole system which is used for airworthiness such as ground control stations (GCS), mobile devices, communication links, etc. Moreover, the terms such as Remotely Piloted Aircraft (RPA), Remotely Piloted Aircraft System (RPAS) and Remotely Piloted Vehicle (RPVs) are also used to denote a UAS. A similar term “drone” is used to denote an autonomously or remotely guided vehicle. According to this definition, drones cover not only UAVs but also other remotely controlled devices such as remotely operated underwater vehicle (ROV). In other words, a UAV may be considered a drone, but a drone does not have to be a UAV [13].

Although the digital forensic investigation of UAVs is crucial for providing security and accountability related to the use of these systems, there are only few academic works focusing on this topic [14, 15, 16, 17, 18, 19].

The control technology embedded inside the Parrot Ar.Drone was investigated by Bristeu and others [20]. It was shown that the Parrot Ar.Drone has a main board embedded with a Parrot P6 processor (32-bit ARM9-core running at 468 MHz), a navigation board embedded with a 16-bit PIC microcontroller running at 40 MHZ, a Wi-Fi chip, a camera, ultrasonic sensors, accelerometers, gyroscopes and a GPS chip. The embedded P6 processor runs with a Linux based real-time operating system. Even though the Parrot Ar.Drone was one of the most popular UAVs at the time, its technology is considered inferior today.

Samland and others, analyzed the security threats of UAVs by using the Computer Emergency Response Team (CERT) taxonomy [19]. They examined the hardware and software components of the four popular drones of the time. They revealed the vulnerabilities of these components. They specifically investigated three different scenarios: "Hijacking the Ar.Drone", "Interception of the video signals of the Ar.Drone" and "Manual tracking of persons using the Ar.Drone". Their work is one of the first attempts in the field, however, as in every field of technology, the UAV technology has been advancing and some of the valuable information given in their work is now out of date. The technology of the UAVs used for this research is out of date and their UAVs are not on the market anymore. Therefore, the techniques used in this study is not applicable for the security threat analysis of the currently used UAVs. The UAVs that are used today have different

and more complicated communication links. In the paper they benefit from the security weaknesses of known network protocols such as FTP and UDP protocols, however, UAVs of our days have their own proprietary communication protocols. For this reason, the vulnerabilities of the UAVs mentioned in their work do not exist on the UAVs used today.

The digital forensic analysis of a Parrot Bebop UAV was conducted by Horsman [15]. Parrot Bebop UAV was one of the most popular drones of 2015. The four main phases of their UAV forensic investigation implementation were identified as "Acquisition of data", "Establishing Flight Data", "Media Taken by the Device" and "Establishing Ownership". They established a wireless network connection to the UAV and, by using Telnet and the File Transfer Protocol (FTP), they were able to access the hidden folders in the UAV which contained evidential information such as flight log files.

Kovar presented the forensic analyses of both the DJI Phantom II and DJI Phantom III model UAVs [17]. He showed that DJI Phantom III contains two types of flight log files. One of these log files is created by the app on the mobile devices that are used to remotely control the UAV and the other log file is stored inside the 4 Gb micro SD card that is located at the bottom of the main board of the UAV. These log files are encrypted or obfuscated and cannot be read directly.

Clark and others performed Digital Forensic Investigation of DJI Phantom III [14]. In their research, they ascertain that DJI Phantom III series UAVs store two kinds of log files. One of these files is created by "DJI Go" Android application and stored on the Android device that is used for controlling the UAV. The other log file is stored on the UAV's internal nonvolatile storage. They correlate both of these log files and reveal that these log files are one to one match. In their research, they emphasize that both of these log files could be used as evidence in front of the court.

The digital forensic investigation of the DJI Phantom II model UAV was performed by Maarse and Sangers [18]. In their work, they focused on retrieving positional data and sequence work to build the flight path of the UAV. They used the flight logs stored on the remote controller of the UAV to retrieve the flight path. The flight log contains the coordinates of the

UAV's home point, the altitude of the UAV and the coordinates of the waypoints. All of these artifacts are stored in 16-bit character strings with UTF-16 little endian encoding.

Jain and Others proposed a UAV Digital Forensic Investigation Framework [16]. Their framework consists of twelve linear phases. Their framework contains Preparation, Identification, Class Identification, Weight Measurement, Check for Customization, Fingerprint, Bluetooth, Wi-Fi, Memory Card, Geo-Location, Onboard Camera and Documentation phases. They tested their framework on five commercial UAVs.

3. METHODOLOGY

In this research, we focus on the forensic analysis of a captured UAV. The UAV could be a suspect UAV that is captured by security forces by being shot by a shotgun (or by using any anti-UAV technique) or it could be a UAV that has crashed into a private property. In order to investigate a UAV forensically, its hardware and software components should be identified and investigated. Besides the investigation of the UAV components, collecting evidence, providing chain of custody and media/artifact analysis are important parts of the forensic investigation.

DJI Phantom III Professional packs all major parts required in a UAV into a small commercial drone. Furthermore, terrorist groups, such as ISIS, has been reported to use this UAV actively [24]. The use of the DJI Phantom III Professional UAV has been detected in several illegal activities such as bomb dropping, remote surveillance, plane watching, etc. For all these reasons, we decided to work on the forensic investigation of the DJI Phantom III Professional UAV in this study.

There has been no standardized investigation framework for the digital forensic investigation of a UAV at the time of this study. There is only one proposed framework [16] for the digital forensic investigation of UAVs in the literature. The proposed framework [16], has a complex structure and is highly dependent on platform types. To eliminate these deficiencies, we propose a UAV digital forensic investigation framework. And then we apply our proposed framework to the forensic investigation of the DJI Phantom III UAV and present our findings in detail.

3.1. UAV Digital Forensics Investigation Framework

In order to disclose any evidence to the court and get it approved, a standardized, or at least acceptable, investigation framework should be used by the investigator. There are numerous kinds of UAVs available in the market and each company uses different hardware and firmware packages. For this reason, although it is difficult to create a single tool for investigating all UAVs, finding a general investigation framework for all kinds of UAVs is a reasonable solution. With this work, we propose a seven-phased framework for the digital forensic investigation of UAVs. An outline of our framework is given in Table 1. Furthermore, we apply our framework to the forensic investigation of a sample UAS, namely the DJI Phantom III Professional drone. We explain our findings on DJI Phantom III Professional in detail in the later sections of the paper. We explain in detail the seven phases of our proposed framework in the rest of this section.

Table 1. Proposed Seven-Phased UAV Investigation Framework

UAV FORENSIC INVESTIGATION PHASES
1. Preparation
2. Scene Control
3. Customization Detection
4. Data Acquisition
5. Evidence Authentication
6. Evidence Examination
7. Presentation

3.1.1. Preparation Phase

An embedded system is a special-purpose computer system designed to perform one or a few dedicated functions. In this respect, MP3 players, mobile phones, PDAs, telemetric systems such as car navigation systems, etc., are all considered embedded systems [25]. Similarly, UAVs are also embedded systems. As it is the case with all embedded devices, the digital forensic investigation of UAVs requires special knowledge and preparation

due to the huge diversity of UAV systems. A forensic investigator has to follow the developments in UAV systems available in the market and have knowledge about both their firmware and hardware components. An undue response on the incident scene could cause irreversible damage to the evidence. To avoid any data loss, the investigator should have knowledge about hardware and software properties of the specific UAV that is investigated.

3.1.2. Scene Control Phase

All kinds of investigation processes that take place on the incident scene form the scene control phase of the digital forensic investigation. During this phase, the investigator should take into consideration any equipment dropped from the UAV during the incidence. Moreover, maintaining chain of custody and protection of evidence from being altered is crucial in this phase. If only the UAV is captured and not the remote control unit, a circle with a radius of the range of the UAV should be explored to find the remote control unit and the owner of the UAV.

3.1.3. Customization Detection Phase

A UAS could be modified to perform specific missions. A forensic investigator should detect these modifications and create a report to be presented to the court. Possible modifications to a UAS could include the following:

a. Range extender usage for flying to longer distances,

b. Battery upgrades for increased flight time,

c. Attaching dropping gear for smuggling and dropping prohibited items to prisons,

d. Camera upgrades for surveillance,

e. Adding autopilot software for pilotless and critical missions such as flying over military units,

f. Deployment of explosives for terrorist activities,

g. Gun mounting for terrorist activities.

3.1.4. Data Acquisition Phase

The Data Acquisition phase of the digital forensic investigation is probably the most important phase in that it involves the collection of all evidence data based on approved forensic techniques. In this phase, all volatile and non-volatile data, such as network based data, live response data, and removable media evidence, should be acquired. In compliance with the "Avoiding Adding Data" principle of digital forensics [26, 27], a write blocker should be used during this phase. Moreover, the investigator should pay attention to the existence of any anti-forensics software laid dormant on the UAV.

3.1.5. Evidence Authentication Phase

Evidence authentication phase is significant for the approval of the collected evidence before the court. During the whole investigation process, the commonly accepted principles of digital forensic investigation, such as "Prevention of Data Loss", "Avoiding Adding Data" and "Chain of Custody" [26, 27], should be taken into consideration. Moreover, the forensic investigation process should be performed on the "Working Copy" of the "Best Copy" that belongs to the original evidence. In the following sections, we explain the evidence authentication techniques that we used during the forensic investigation of our sample UAS.

3.1.6. Evidence Examination Phase

In the evidence examination phase, the investigator probes into all data that is acquired from the UAS. The investigator tries to find evidence about specific cases. The rebuilding of the flight path for a suspicious flight is of vital importance as evidence before the court of law. Also, any kind of video or image file could be used as an evidence.

3.1.7. Presentation Phase

Last but not least, the presentation phase is the final step of a digital forensic investigation. All efforts made during the whole investigation process should be explained in detail, ready to be presented before the court. A report should be prepared that presents all evidence about the case at hand. While preparing the report, one should always keep in mind that the judge, or the jury, in the court does not have to be a technical person and therefore a plain and understandable language must be used.

4. Forensic Investigation of DJI Phantom III Professional

We applied our framework on the forensic investigation of the DJI Phantom III Professional Drone, the DJI Phantom III Professional Remote Controller and their associated app running on an Android tablet (Samsung Galaxy Tab 3 Lite). In the rest of this section, we explain the seven phases of our digital forensic investigation framework applied to this tested UAS.

4.1. Preparation Phase

The sample UAS used for this study (DJI Phantom III Professional) consist of two main components, aircraft and ground control station (GCS). From the outer appearance, the aircraft has four propellers, 4480mAH Li-Po intelligent battery, gimbal, 4K resolution camera, micro SD-Card mount on gimbal, a USB port, and Wi-Fi antennas. Inside the aircraft, there are four brushless motors and four electronic speed control units, one for each propeller, a single main board which contains all the modules of Inertial Measurement Unit (IMU), a gyroscope unit, a GPS sensor, a speed controller unit and a Wi-Fi unit. Last but not least, on the bottom of the aircraft, there is a 4GB capacity SD-card, which is used for recording all the flight data. The ground control station consists of a remote controller and a mobile device which runs the "DJI Go" application. The mobile device is connected to the remote controller through a USB port and the remote controller communicates with the aircraft via the Lightbridge protocol on the 2,400-2483GHz frequency [28].

The sample UAS uses Open WRT 14.07 "Barrier Breaker r2879, 14.07" built for the "ar71xx/generic" operating system, on both the aircraft and the remote controller. This firmware is a Linux based operating system used for embedded systems [29, 30]. Consequently, the OverlayFS, tmpfs, SquashFS, JFFS2, UBIFS, ext2 and mini_fo file systems, could be contained in the UAS. The DJI Go application runs on both Android and IOS devices. In addition to the drone's internal SD-card, the DJI Go application creates a very detailed flight record and stores it on the mobile device.

4.2. Scene Control Phase

Even though this phase is within other criminal discipline's field of interest, a digital forensic examiner should investigate the incidence area. On the incident scene, the examiner should search for any dropped items from the UAV. Since we conducted the flights in the scope of this paper, no dropping off item is detected. Since our sample UAV has an up to 5 kilometers of range, a circle whose center is the incident scene and with a radius of 5 kilometers is drawn. The remote controller and the owner of the UAV are probably located in this area.

4.3. Customization Detection

The investigator should take into account any customizations on the UAS. By the reason that our sample UAV contains no customization, we do not locate any customization.

4.4. Data Acquisition

As a first step in the data acquisition phase, in accordance with the "Prevention of Data Loss" and "Avoiding Adding Data" principles of digital forensic investigation, we applied the factory reset procedures to both the drone and the Samsung Galaxy Tab 3 Lite tablet before performing our tests. We formatted the drone by using the DJI Go application. This process deleted all of the nonvolatile files from the internal storage of the drone. Then we formatted the Android tablet to its factory settings by using its booting menu. After formatting, we updated the device to the latest Android version and the latest version of the DJI Go application. As a final precautionary step, we wiped the SD card located on the gimbal and that is used for video and picture storage. For this wipe operation, we used the "Disk Dump (dd) utility" with the "zero of" command which fills the whole disk with zeroes during the wipe procedure. We formatted the disks to the FAT32 file system.

After wiping and formatting the UAS to its factory settings, we planned and conducted ten different flights with it. We conducted these flights on different places, on different days and at different times of the day. We recorded the date, time, location and flight pattern information for these flights.

After conducting the flights, we started the data acquisition phase of our forensic investigation. During the data acquisition phase, we used the FTK Imager tool for getting the physical image. To follow the "preventing adding data" principle a "write-blocker" should be used. Firstly, image of the tablet is generated. The image is labeled as "*Evidence_storage_001*" Secondly drone's internal storage is imaged. The image is labeled as "*Evidence_storage_002*". Lastly, the same process applied to the SD card stored on the gimbal and labeled as "*Evidence_storage_003*". All of the images are copied and the investigations are conducted on the best working copy of the images.

4.5. Evidence Authentication Phase

This phase should be conducted right after the "data acquisition phase". In this phase, the "md5sum" utility was used for MD5 hash generation. The MD5 hash values of the Android device, the internal SD card of the aircraft and the SD card stored on the gimbal were calculated. The hash values which are created with the "md5sum" utility and the "FTK Imager" tool were compared and verified to be equal. Thus, the evidence was verified to be authentic. The evidence Authentication data is shown on Table 2.

Table 2. Evidence Authentication Data

EVIDENCE	EVIDENCE MD5 HASH (with FTK)	IMAGE OF THE EVIDENCE MD5
Evidence_storage_001	702aefc3bc17a7ae 0ae983021d3e0685	702aefc3bc17a7ae 0ae983021d3e0685
Evidence_storage_002	1309901b969b1bf7 898c9c1711fb2fd0	1309901b969b1bf7 898c9c1711fb2fd0
Evidence_storage_003	f5d18bd470399ac5 12392ef0771be315	f5d18bd470399ac5 12392ef0771be315

4.6. Evidence Examination Phase

During the Evidence Examination Phase, all of the examinations were conducted on the best working copy of the evidence images to prevent any alteration of the data.

We were able to locate three different digital pieces of evidence on the sample UAS. The first one of these evidences was a ".TXT" extended file that is created by the "DJI Go" application. This text file was stored on the smart device which is used for controlling the drone. The second evidence was a ".DAT" extended file that was created by the drone itself. This file was stored in the drone's internal memory. Finally, the third evidence found is the EXIF data files that are stored in the drone's internal memory for each picture taken by the drone. Finally, at the end of the "Evidence Examination Phase", we were able to regenerate the flight path of the flight by using GPS coordinates information located on the flight log files. We explain the details of these artifacts in detail below.

4.6.1. *DJI Go .txt File*

During the investigation of the Android tablet image, several directories were detected that pertain to DJI. The investigation on the Android tablet was mainly focused on these directories. In the data/dji.pilot/DJI/FlightRecords directory of the Android tablet, the file named as DJIFlightRecordyYYYY-MM-DD_[HH-MM-SS].txt caught our attention. This text file could not be opened by any text editor, however, we were able to convert this file to a readable .csv file using some online tools (https://airdata.com).

4.6.2. *.dat File Created by the DJI Drone*

DJI Phantom III drones contain a micro SD-Card with 4 GB storage capacity located on the bottom of the main board. To access this storage hardware, the aircraft had to be laid open and the main board must be removed from the drone. The SD-Card was glued to the card slot, therefore we had to scratch the glue to remove the SD-Card. After doing this, we took the image of the SD-Card to prevent any loss of data and then copied the image. We inspected this copy with scrutiny. During our inspection, we detected 10 files, named as FLY***.DAT. The numbers *** in the file

names were consecutive numbers. We detected that these .dat extended files were in binary format. We used the tool DatCon (https://datfile.net/) to convert these .dat extended flight records into human readable .csv files.

4.6.3. *EXIF Data File*

DJI Phantom III drones store all their recorded videos and taken pictures in an SD-Card located in the gimbal. We exported a few pictures from the image of the SD-Card to analyze the metadata of these pictures. At first glance, we saw that the drone stores pictures as .jpg extended files and videos as .mov extended files. We read the EXIF headers of the images using the tool "ExifTool" and thus we were able to detect a lot of valuable information such as the creation dates of the images and the GPS locations where the images were taken.

4.7. Presentation Phase

Since the judge in the court is not necessarily a technical person, a plain and understandable language must be used in the forensic investigation report. In the report, all the steps of the investigation should be described properly. An example report template that could be used to present findings in front of the court is shown on Figure 1.

5. Testing and Comparison

There is only one proposed framework for digital forensics investigation of UAVs at the time of this study [16]. Digital forensics investigation of the sample UAS was conducted according to both our proposed framework and the framework proposed by Upasita et al [16].

5.1. Testing the Proposed Seven-Phased UAV Investigation Framework

Our proposed Seven-Phased UAV Investigation Framework was tested with the DJI Phantom III Professional UAS. During the investigation process, we always kept in mind the well-known digital investigation principles, such as preserving digital evidence, preserving chain of custody, avoiding adding data and documenting actions [10].

<table>
<tr><td colspan="3">Suspicious Incident :</td><td>Incident Date :</td></tr>
<tr><td colspan="4">Incident Scene Description and GPS Position:</td></tr>
<tr><td colspan="4">Incident Scene Investigation :</td></tr>
<tr><td colspan="4">Detected Customizations on Suspicious UAV :</td></tr>
<tr><td colspan="4">Evidence Acquisition and Authentication :</td></tr>
<tr><td colspan="2">Evidence :</td><td colspan="2">Acquisition Date and Time :</td></tr>
<tr><td colspan="2">Evidence Hash Value :</td><td colspan="2">Image of The Evidence Hash Value:</td></tr>
<tr><td colspan="2">Evidence :</td><td colspan="2">Acquisition Date and Time :</td></tr>
<tr><td colspan="2">Evidence Hash Value :</td><td colspan="2">Image of The Evidence Hash Value:</td></tr>
<tr><td colspan="4">Evidence Examination and Findings :</td></tr>
<tr><td>Evidence :</td><td>Flight Date and Time :</td><td colspan="2">Flight Duration :</td></tr>
<tr><td colspan="2">The Closest GPS Position to Incident Scene :</td><td colspan="2">Altitude of the Closest GPS Position to Incident Scene :</td></tr>
<tr><td colspan="2">Distance Between The Closest GPS Position and Incident Scene :</td><td colspan="2">Duration on the Closest GPS Position :</td></tr>
<tr><td colspan="4">Examiners Judgement :</td></tr>
</table>

Figure 1. An Example Report Template

When the phases of our framework are applied in a forensic investigation, our framework significantly helps the investigators to detect any evidences in the incident scene (i.e. dropped items), locate any customizations for specific missions, present the data acquisition, authenticate the acquired data (crucial for proving that the evidence is authentic), analyze the acquired data with proper methods and lastly present all the findings in front of the court.

As a result of our investigation process, we were able to acquire evidence related to a specific suspicious incident to present them in front of the court. As it is mentioned earlier, we were able to locate three kinds of forensic artifacts on the sample UAS. At the end of our investigation, we were able to regenerate the flight path of any suspicious flight, thanks to the GPS coordinates information that was included in the obtained evidence.

5.2. Results of the Framework Proposed by Upasita et al.

The investigation by Upasita et al. is conducted according to their proposed framework in twelve steps. The twelve phases of their framework and the result of each phase are given below.

1. Preparation Phase: Assessment of the risks, threats, and vulnerabilities of the sample UAS are made. The sample UAS has a range of 3.1 nm (approximately five kilometers) with 25 minutes of flight time. The maximum operating altitude of the sample UAV is 19685 ft (6000m). The sample UAS can run some autopilot applications to conduct some specific missions.

2. Identification/Collection Phase: All data contained by the sample UAS is acquired by the techniques mentioned in Section 4.4 Data Acquisition.

3. Identify Class/Category Phase: The weight of the sample UAS is 1280 grams. According to UAV regulations of the Directorate General of Civil Aviation in Turkey, our sample UAS is in the UAV-0 class. According to the regulation, all UAVs in the UAV - 0 class have to be registered.

4. Measure Weight Phase: As it is mentioned in the previous phase, our sample UAS 1280 grams and it has to be registered.

5. Check for the Customization Phase: Same as our proposed seven-phased UAV investigation framework, we check for any customization on the sample UAS, and as it is mentioned hereinbefore we cannot locate any customization.

6. Fingerprint Phase: Since detecting and investigating the fingerprints located on a suspicious UAV is within the scope of not digital forensics but other criminal disciplines, we do not investigate the fingerprints.

7. Bluetooth Phase: The sample UAS does not have any Bluetooth modules.

8. Wi-Fi Phase: Even though the sample UAS communicates on the Wi-Fi frequency, it uses a proprietary protocol called "Lightbridge" and the communication between the aircraft and the remote controller cannot be exploited by ordinary Wi-Fi chips.

9. Memory Card: Our sample UAS has a 16GB capacity micro SD-Card located on the gimbal (camera mount of the UAV). The captured images and the videos are located on this storage equipment.

10. Geo-location Phase: The sample UAS has both GPS and GLONASS satellite positioning systems. Besides, it has a vision positioning system for flying in indoor areas.

11. Camera Phase: The sample UAS has a 4096 x 2160p (UHD) resolution camera on board. The camera is located on the gimbal which helps keep the camera stabilized during the flight.

12. Documentation Phase: The findings of the investigation are documented, corresponding with the report template which is mentioned hereinbefore.

5.3. Framework Comparison

Both our framework and the framework by Upasita et al. are implemented on the sample UAS, namely DJI Phantom III Professional. We have seen that the "Preparation" and "Customization Detection" phases are the common phases in both frameworks.

As a result of our comparison of both frameworks, we identify some differences. The most significant difference is that while our investigation

framework is related to the investigation of the digital data stored on the suspicious UAV, the other framework mainly focuses on the hardware specifications of the suspicious drone. The framework proposed by Upasita et.al only investigates the Wi-Fi and Bluetooth modules of the UAV, however, some of the new generation, bigger and more complex UAVs use different communication frequencies and protocols for communicating at longer distances. Besides, our framework covers the investigation of the whole UAS and not just the aircraft, whereas the framework offered by Upasita et al. only investigates the aircraft and does not deal with the data stored on the GCS. The main purpose of our framework is to regenerate the flight path of a captured suspicious drone. We can achieve this in our framework thanks to the analysis results of the flight logs and other artifacts found on the UAS. The framework proposed by Upasita et al. focuses on finding evidence only in the captured image and video files.

In a forensic investigation, the investigator has to prove that, the evidence presented in front of the court are authentic. In the data authentication phase of our framework, we prove that we conduct our investigations on the authentic evidence. The framework offered by Upasita et al. does not prove the authenticity of the presented evidence.

The framework proposed by Upasita et al. detects the classification/category of the suspicious UAV. The detection of the classification/category of suspicious UAV helps the investigator to find the regulations related to the UAV. Most countries have regulations for registering UAVs according to their classification. This phase helps the investigator to identify the owner/pilot of the UAV. Since that our framework mainly focuses on the digital data, and owner/pilot identification of the UAV is in the scope of different criminal disciplines, this feature is not contained by our proposed framework.

Table 3. Comparison of the Proposed Framework and the Framework by Upasita et al.

Feature	Seven-Phased UAV Investigation Framework	Framework by Upasita et al.
Preparation Before Investigation	✓	✓
Customization Detection	✓	✓
Digital Data Investigation	✓	**X**
Hardware/Gear Investigation	**X**	✓
GCS Investigation	✓	**X**
Flight Path Regeneration	✓	**X**
Preserving Data Authentication	✓	**X**
Classification/Category Detection	**X**	✓

6. CONCLUSION, RECOMMENDATIONS AND FUTURE WORK

With this research, we aimed to create a framework for systematically detecting and classifying any criminal activity conducted with UAVs. The massive increase in the usage of UAVs has also led to a dramatic increase in the illegal usage of these devices. The illegal usage of UAVs has revealed a legal loophole in the current aviation regulations due to the lack of sufficient information and existing standards on the forensic investigation of these incidents.

We proposed a seven-phased UAV digital forensics investigation framework and tested its efficacy by implementing it on a sample UAS. We experienced that our framework works successfully and it significantly helps with the forensic investigation of UASs in a systematic manner. We believe that our proposed framework contributes to digital forensics investigators on the investigation of UAVs.

REFERENCES

[1] Clarke, R. (2014). "Understanding the Drone Epidemic". ***Computer Law & Security Review***, vol.30, no.3, pp.230-246.

[2] Bellamy, W. (2017). "US Now Has 60,000 Part 107 Drone Pilots", Retrieved from http://www.aviationtoday.com/2017/09/07/us-now-60000-part-107-drone-pilots/ (Access Date: 16.04.2018).

[3] Steve, D. (2017). "There are Over 770,000 Registered Drone Owners in The US", Retrieved from https://www.engadget.com/2017/03/28/there-are-over-770-000-registered-drone-owners-in-the-us/(Access Date: 16.04.2018).

[4] FAA Aerospace Forecasts 2018 - 38. pp. 39 - 45.

[5] Cracknell, A. P. (2017). "UAVs: Regulations And Law Enforcement", ***International Journal Of Remote Sensing***. vol.38, no.8-10, pp.3054-3067.

[6] Ravich, T. M. (2015). "Courts In The Drone Age", ***Northern Kentucky Law Review,*** vol.42, no.2, p.161.

[7] Loffi, J., Wallace, R. J., and Ison, C. S. (2016). "Analysis of the Federal Aviation Administration's Small UAS Regulations for Hobbyist and Recreational Users", ***International Journal of Aviation, Aeronautics, and Aerospace***. vol.3, no.1, p.3.

[8] Buckley, L. E. (2014). "Recreational UAVs: Going Rogue with Pennsylvania's Strict Products Liability Law Post-Tincher", ***University Of Pittsburgh Journal Of Technology Law & Policy,*** vol.15, p.243.

[9] Maddox, S., and Stuckenberg, D. (2015). "Drones In The U.S. National Airspace System: A safety and security assessment", ***Harvard Law School National Security Journal***.

[10] Valjarevic, A., and Venter, H. S. (2016). "Introduction of concurrent processes into the digital forensic investigation process", ***Australian Journal Of Forensic Sciences,*** vol.48, no.3, pp.339-357. doi:10.1080/00450618.2015.1052754.

[11] Valavanis, K. P., and Vachtsevanos, G. J. (2014). ***The handbook of Unmanned Aircraft Vehicle***. Springer.

[12] U.S. Army (2005) Unmanned Aerial System (UAS) Roadmap 2005-2030.

[13] Giones, F., and Brem, A. (2017). "From Toys to Tools: The Co-Evolution of Technological and Entrepreneurial Developments in the Drone Industry", ***Business Horizons,*** vol.60, no.6, pp.875-884. doi:10.1016/j.bushor.2017.08.001.

[14] Clark, D., Meffert, C., Baggili, I., and Breitinger, F. (2017). "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III", ***Digital Investigation,*** vol.22, pp.3-14. doi:10.1016/j.diin.2017.06.013.

[15] Horsman, G. (2016). "Unmanned Aerial Vehicles: A Preliminary Analysis of Forensic Challenges". ***Digital Investigation,*** vol.16, pp.1-11.

[16] Jain, U., Rogers, M., and Matson, E. T. (2017, March). "Drone Forensic Framework: Sensor And Data Identification and Verification", ***In Sensors Applications Symposium (SAS)***. pp. 1-6.

[17] Kovar, D., Dominguez, G., and Murphy, C. (2016). "UAV (aka drone) Forensics", ***SANS DFIR summit*** in Austin, TX July, 7.

[18] Maarse, M., Sangers, L., van Ginkel, J., and Pouw, M. (2016). "Digital forensics on a DJI Phantom 2 Vision+ UAV", ***MSc System and Network Engineering,*** University of Amsterdam.

[19] Samland, F., Fruth, J., Hildebrandt, M., Hoppe, T., and Dittmann, J. (2012, January). "AR. Drone: security threat analysis and exemplary attack to track persons. In Intelligent Robots and Computer Vision XXIX: Algorithms and Techniques (Vol. 8301, p. 83010G)", ***International Society for Optics and Photonics***.

[20] Bristeau, P. J., Callou, F., Vissiere, D., and Petit, N. (2011). "The Navigation and Control Technology Inside the Ar. Drone Micro UAV", ***IFAC Proceedings Volumes***. vol.44, no.1, pp.1477-1484.

[21] Bunker, R. J. (2015). "Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications", ***Strategic Studies Institute, US Army War College,*** pp.13-15.

[22] Lim, K. S., and Lee, S. (2008, December). "A methodology for forensic analysis of embedded systems", ***In Future Generation Communication and Networking, 2008. FGCN'08. Second International Conference****,* Vol.2, pp. 283-286.

[23] Association of Chief Police Officers (ACPO) (n.d.) "The Principles of Digital Evidence". Retrieved from http://www.computerforensicsspecialists.co.uk/blog/the-principles-of-digital-evidence (Access Date: 29.04.2018).

[24] Kerr, O. S. (2005). "Digital Evidence And The New Criminal Procedure", ***Columbia Law Review****,* Vol.105, No.1 pp.279-318.

[25] DJI Company (2016) DJI Phantom III Professional User Manual

[26] Kciuk, M. (2014, September). OpenWRT operating system based controllers for mobile robot and building automation system students projects realization. ***In Research and Education in Mechatronics (REM), 2014 15th International Workshop***, pp. 1-4. IEEE.

[27] VoidSec. (n.d.). "Hacking The DJI Phantom III", Retrieved from https://voidsec.com/hacking-dji-phantom-3/ (Access Date: 29.04.2018).

[28] Conte, T. M., and Wolfe, A. (2014). "Techniques for Detecting Encrypted Data". U.S. Patent No. 8,799,671. Washington, DC: U.S. Patent and Trademark Office.