THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

UNMANNED AERIAL VEHICLE DIGITAL FORENSIC INVESTIGATION

Master's Thesis

IBRAHIM GULATAS

ISTANBUL, 2018

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES COMPUTER ENGINEERING

UNMANNED AERIAL VEHICLE DIGITAL FORENSIC INVESTIGATION

Master's Thesis

IBRAHIM GULATAS

Supervisor: ASSIST. PROF. SELCUK BAKTIR

İSTANBUL, 2018

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
COMPUTER ENGINEERING

Name of the thesis: Unmanned Aerial Vehicle Digital Forensic Investigation
Name/Last Name of the Student: Ibrahim GULATAS
Date of the Defense of Thesis: 25 May 2018

The thesis has been approved by the Graduate School of Natural and Applied Sciences.

Assist. Prof. Yucel Batu SALMAN
Graduate School Director
Signature

I certify that this thesis meets all the requirements as a thesis for the degree of Master of Arts.

Assist. Prof. Tarkan AYDIN
Program Coordinator
Signature

This is to certify that we have read this thesis and we find it fully adequate in scope, quality and content, as a thesis for the degree of Master of Arts.

Examining Comittee Members	Signature
Thesis Supervisor Assist. Prof. Dr. Selcuk BAKTIR	----------
Member Assist. Prof. Dr. Tarkan AYDIN	----------
Member Assoc. Prof. Dr. Siddika Berna Ors YALCIN	----------

ACKNOWLEDGMENTS

First of all, I want to thank all of the instructors of Computer Engineering department of Bahcesehir University, especially my thesis supervisor Assist. Prof. Selcuk BAKTIR, without their experience, mentorship, background, understanding and helps it was impossible to complete this thesis study.

I would like to thank my "Computer Forensics" lecturer and founder of "DigiSecure" Halil Ibrahim SARUHAN, who gave me the idea of working on this innovative and promising subject as a Master's Thesis.

Finally, I would like to appreciate my dear wife Yasemin GULATAS for her endless support not only in all phases of thesis program, but also in all of our life.

ISTANBUL 2018, Ibrahim GULATAS

ÖZET

İNSANSIZ HAVA ARAÇLARI ADLİ BİLİŞİM İNCELEMESİ

İbrahim GÜLATAŞ

Bilgisayar Mühendisliği

Tez Danışmanı: Yrd. Doç. Dr. Selçuk BAKTIR

Mayıs 2018, 44 sayfa

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 incelemeler sonucunda incelenen insansız hava aracında üç adet dijital delil tespit edilmiştir. Bulunan bu delillerin iki adedi uçuş kayıt dosyası, diğeri ise araçta bulunan kamera tarafından çekilen görüntü dosyalarındaki metadata bilgileridir. Örnek sistemde bulunan iki adet uçuş kaydının derinlemesine incelemesi yapılmış, incelemeler esnasında bu dosyaların DJI firmasına ait özgün bir formata sahip olduğu tespit edilmiştir. Dosyalar üzerinde yapılan incelemeler ve tersine mühendislik işlemleri sonucunda, dosyaların yapısı tam olarak çıkarılmış ve insansız hava aracının gerçekleştirdiği uçuşlara ait GPS koordinatları ve uçuş haritaları elde edilmiştir. Yapılan tüm incelemelerin soncunda bu çalışma kapsamında önerilen yedi aşamalı inceleme sisteminin, araştırmacılara insansız hava araçlarının adli bilişim incelemelerinin, sistematik bir şekilde icra edilmesi açısından faydalı olduğu değerlendirilmiştir.

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

ABSTRACT

UNMANNED AERIAL VEHICLE DIGITAL FORENSIC INVESTIGATION

Ibrahim GULATAS

Computer Engineering

Thesis Supervisor: Assist. Prof. Dr. Selcuk BAKTIR

May 2018, 44 pages

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, a seven-phase UAV digital forensics investigation framework is proposed to standardize the investigation process for UAVs. The framework was tested 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 these 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. The log files of the UAV has a proprietary data structure. By reverse engineering this data structure, the flight paths for all the flights taken by the investigated UAV, could be derived. At the end of the whole investigation process, it is observed that the proposed seven-phased investigation framework works successfully and significantly helps with the forensic investigation of UASs in a systematic manner.

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

CONTENTS

TABLES

FIGURES

ABBREVIATIONS

ACPO	:	Association of Chief Police Officers
CAA	:	Civil Aviation Authority
CERT	:	Computer Emergency Response Team
DOD	:	U.S. Department of Defense
EASA	:	European Aviation Safety Agency
FAA	:	Federal Aviation Administration
GCS	:	Ground Control Station
IMU	:	Inertial Measure Unit
IOCE	:	International Organization on Digital Evidence
IOT	:	Internet Of Things
OSD	:	On Screen Display
RPA	:	Remotely Piloted Aircraft
RPAS	:	Remotely Piloted Aircraft System
RPV	:	Remotely Piloted Vehicle
S-UAS	:	Small Unmanned Aerial System
SWGDE	:	Scientific Working Group on Digital Evidence
UAS	:	Unmanned Aerial System
UAV	:	Unmanned Aerial Vehicle

1. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) have become increasingly popular to use, with a wide range of usage areas, throughout the world. Actually, the first usage of UAVs dates back to 19th century. "On 22 August 1849 Austria launched the first air raids in history to the Venice (Clarke, 2014)". According to to the documentary "A Wind And A Prayer" (2005), Austria beleaguered the Venice both from land and sea, but their siege artillery couldn't get close enough to bear fire. To cope with the problem "Austria launched the first air raids in the history by unmanned balloons which floated over Venice charged with bombs and shrapnel". On the air raid, there were approximately 200 unmanned balloons which carry 33 pounds of explosives. 2 days after the air raid Venice was surrendered. The second known usage of the UAVs is at the World War II in 1944. Japanese also used unmanned balloons which carry bombs to fly over the western United States.

While the first UAVs was used as early as on 1849, UAVs have found widespread usage in only recent years. Since the 19th century, as in every field of the technology, UAVs are changed and improved a lot. Today it is easier to own and easier to fly a UAV. A UAV could be bought with 20USD budget and a 10 years old child can fly with it easily. While it gets popular, the term "drone" is generally used for small and commercial ones, nevertheless, UAV term is generally used for bigger UAVs especially used by military forces.

According to Goldman Sachs Drones Report, $100 billion market revenue is expected between 2016 and 2020. By the end of 2017, there are 770.000 hobbyists (Bellamy, 2017) and 80.000 commercial Unmanned Aerial System (UAS) pilots had registered as UAS pilots in the United States (Dent, 2017). By the 2021 it is expected that there will be about 3,5 million units in hobbyists fleet[1]. Both of the Hobbyists and Commercial Fleets forecasted unit numbers by the years are listed in the Table 1.1.

[1] FAA Forecasts 2017-2037

Table 1.1: Total UAS Forecasts

Year	Hobbyists Fleet		Commercial Fleet	
	Million sUAS Units		Million sUAS Units	
	Low	High	Low	High
2016	1,10	1,10	0,042	0,042
2017	1,94	2,31	0,095	0,235
2018	2,37	3,18	0,133	0,445
2019	2,60	3,79	0,173	0,742
2020	2,69	4,15	0,207	1,133
2021	2,75	4,47	0,238	1,616

Source: FAA Forecast 2017-2037

As it becomes easier to fly a UAV and more people able to own a drone, people started to use UAVs for illegal purposes. Some of the illegal usage areas of the UAVs are listed as follows.

i, Terrorism:

The Newsweek article titled "Terrorist Drone Attacks Are Not an 'If' But 'When'." indicates that terrorist groups are using UAVs for their violent acts. They used UAVs for scouting military positions, dropping chemical or explosive packages to attack civilian populations and filming propaganda videos of the military operations.

18 years old college student Austin Haughwout built a UAV with a remotely controlled handgun. He posted his video titled "Flying Gun" on YouTube. On the video, a handgun fixed on a UAV was shot 3 times while UAV was on hover position. The video shows that this kind of weapon can be also developed and used by terrorist groups.

ii,Prisons:

It is detected with the CCTV of the prisons that some organizations deliver drugs, weapons and mobile phones to prisons with UAVs. (Cracknell, 2017)

iii, Plane watchers:

The Federal Aviation Administration (FAA) reported that from August 22, 2015 to January 31, 2016, 600 drones were detected to fly too closely to airports or planes. Crashing a plane with a UAV will result with a huge disaster. UAVs are restricted to fly over 400 feet and five miles of an airport. People are occasionally broke this rule because they are very curious about a flying plane.

iv, Private Life Privacy Violations:

FAA guidelines specify that drones should not be flown over people, stadiums, large crowds and private properties. There are lots of cases in the courts about violating this rule. (Ravich, 2015)

Since the illegal usage UAVs, in violation of the Federal Aviation Administration (FAA) regulations (Hartzler 2018), 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 (Maddox and Stuckenberg 2015). 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.

This study focuses on proposing a framework to be used for digital forensic investigation of UAVs and implementation of this framework to one of the most popular commercial drones on the market. During the implementation of the new method, all of the forensic investigation principals such as preserving digital evidence, preserving the chain of custody, avoiding adding data and documenting actions (Valjarevic and Venter 2016) are kept in mind.

During the implementation of the proposed UAV forensic investigation framework, DJI Phantom III series drones (Standard and Professional) are used for investigation. Even though there are not too many differences between these two drones, the main

difference is their communication links. The standard version of the drone uses Wi-Fi for communication between drone, remote controller and mobile device. On the other hand, the professional version uses a proprietary protocol called "Lightbridge".

According to the FAA records, DJI is the leader company in the commercial UAV business.[2] Their UAVs account for 70% of the commercial UAV market. The DJI Phantom III Professional model UAV was reported to be the best selling drone (Divya 2017) both in 2015 and 2016 (Yue 2016). Besides, 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 for surveillance (Pomerleau, 2017). 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, DJI Phantom III Professional UAV decided as the sample UAS investigate forensically in this study.

UAVs are remote controlled, flying, embedded and Internet Of Things (IoT) devices. For this reason, embedded devices and IoT devices forensic investigation methods are applied to the sample UAS. Its find out that DJI Phantom III uses Linux based "OpenWRT" operating system which is designed for especially embedded devices. Therefore Linux file systems are examined throughly. Moreover, DJI uses proprietary data format. To extract the file structure of these data, reverse engineering techniques are applied to the flight logs of the sample UAS.

As a result of digital forensic investigation of DJI Phantom III, three artifacts were found in different platforms, to present into law court as an evidence. One of the artifacts is found on the mobile device that is used for controlling the aircraft. The other one found on the internal storage area of the drone. The last one is found in the EXIF data of the images taken by the camera located on the drone. At the end of the

[2] DJI (company). (n.d.). In Wikipedia. Retrieved April 29, 2018, from https://en.wikipedia.org/wiki/DJI_(company). (Internet Sources).

investigation flight path of the drone was acquired.

Study structure is as follows: Section 2 covers, review of literature list. Section 3 covers, DJI Phantom III drone review, proposed investigation framework for UAV forensics, data and methods used for digital investigation of Phantom III UAV and forensic artifacts of the sample UAS. Section 4 covers the findings of the digital forensic investigation and data structures of the flight logs which has DJI's proprietary data format. Finally, section 5 covers conclusion, future works and recommendations for researchers and investigators who plan to work with UAVs.

2. LITERATURE REVIEW

2.1 RESEARCH OVERVIEW

Research study started with the investigation of the literature that focuses on "UAV review", "Digital Forensics Investigation", "Mobile Devices Forensics Investigation", "Internet of Things (IoT) Forensics Investigation", Wireless Network Security and Anti-UAV techniques. As an initial step, published papers, articles, online resources and reports were researched. It has been observed that; 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.

This study focuses 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.

Moreover, to prevent illegal usage of the UAVs, this literature research study also focuses that what kind of actions could be done if a UAV is detected on a restricted area or how to take control of a flying UAV. For this section, anti-UAV techniques, wireless network security, wireless network hijacking and UAV hijacking subjects are researched.

2.2 LITERATURE LIST

As an initial step, some of the most popular UAV's user guides, repair guides and hobbyist forums are researched to getting familiar with the hardware components and software packages running on as-UAS. Researches are focused on the DJI's Phantom III

models because DJI drones have been already detected on illegal activities and DJI Phantom III UAVs contain all the major parts of an s-UAS.

2.2.1 General Information About UAVs

Vachtsevanos and Valavanis (2015), defined UAV 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. The related term UAS was first introduced by the "U.S. Department of Defense (DoD)", which was flowed by FAA and "European Aviation Safety Agency (EASA)" (U.S. Army 2005). 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 (GSC), 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.

Parker (2018), reveals the differences between terms of drone and UAV. The definition of the drone is any kind of 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, any UAV may be considered as a drone, but any drone may not a UAV (Gregg 2018). However, in the general concept, UAV is used for military vehicles and drone is used for personal and commercial vehicles.

Classification of the UAVs is the one of the main concern of the governments and some organizations in terms of aviation security. It takes an important place to classify the UAVs, with regards to preparing regulations about the rights and responsibilities of the owners and pilots. Most of the analysts classified the UAVs according to different parameters. Weight, size, flight altitude, equipment on board, wingspan, endurance and usage areas of the UAVs are used for classifications. Directorate General Of Civil Aviation - Turkey (2017) classifies the UAVs according to their maximum takeoff weight. The classification attributes are shown on Table 2.1. According to the regulation

all both UAV-0 and higher class UAVs and their pilots have to be registered. Besides, all of the UAV-1 must have a flight recorder on the aircraft or ground control station.

Table 2.1: Directorate General Of Civil Aviation - Turkey UAV Classification

UAV CLASS	MAXIMUM TAKEOFF WIGHT (kilograms)
Unclassified	0 - 0,5
UAV-0	0,5 - 4
UAV-1	4 - 25
UAV-2	25-150
UAV-3	More than150

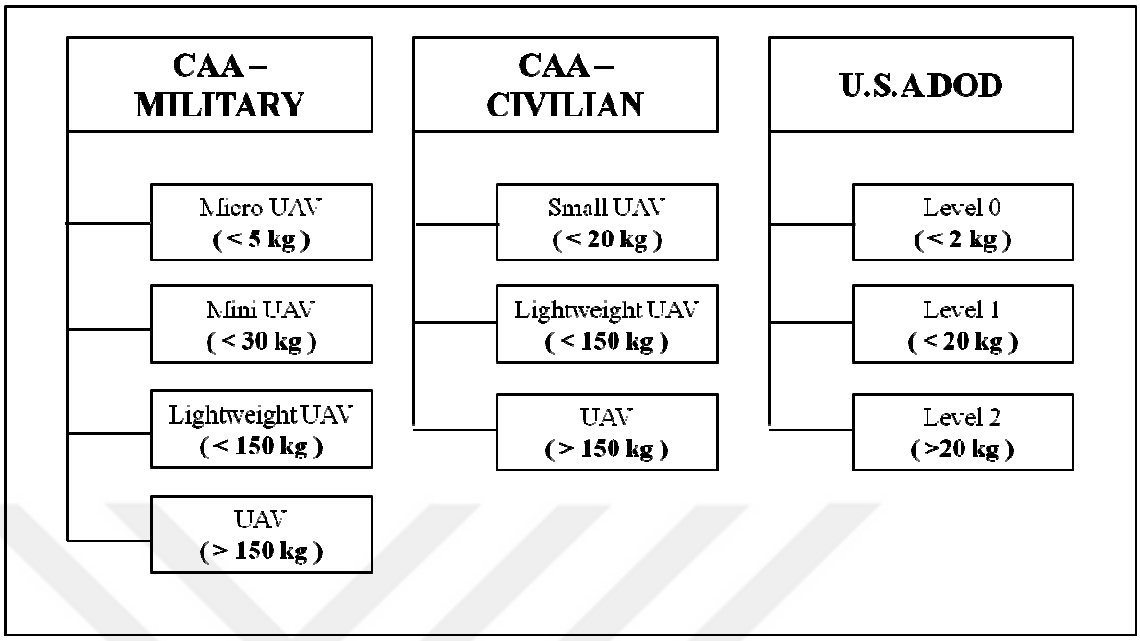
Moreover, The U.S.A DoD (2011) classified UAVs according to different parameters. Table 2.2 shows the U.S.A UAS classification. Civil Aviation Authority (CAA) classified the civilian and military UAVs according to their maximum takeoff weight. Figure 2.1 shows the comparison of CAA and U.S. DoD classification.

Table 2.2: The U.S. DoD UAS classification

<table>
<tr><th>UAS Category</th><th>Max Gross Takeoff Weight (Lbs)</th><th>Normal Operating Altitude (Ft)</th><th>Airspeed (knot)</th></tr>
<tr><td>Group 1</td><td>< 20</td><td>< 1200 above ground level (AGL)</td><td><100</td></tr>
<tr><td>Group 2</td><td>21-55</td><td><3500 AGL</td><td rowspan="2"><250</td></tr>
<tr><td>Group 3</td><td>< 1320</td><td rowspan="2"><18000 mean sea level (MSL)</td></tr>
<tr><td>Group 4</td><td rowspan="2">>1320</td><td rowspan="2">Any Airspeed</td></tr>
<tr><td>Group 5</td><td>>18000 MSL</td></tr>
</table>

Source: Eyes Of The Army - U.S. Army Roadmap for UAS 2010-2035.

Figure 2.1: UAV Classification Comparison



Source: Review of the Elementary Aspect of Small Solar-powered Electric Unmanned Aerial Vehicles.

McKibben and Sanchez (2015), point out the criminal uses of UAVs. When a small UAV crashed into the lawn of the White House, it became prominent that how easily drones could fly into restricted areas. Besides lots of drone flights have been detected on no fly zone such as nuclear power plants. In the article, it is emphasized that terrorist groups such as ISIS and Hezbollah procured drones and uses it for reconnaissance and aid in launching ground attacks. UAVs are detected to used for smuggling. Individuals used UAVs to deliver mobile phones, marijuana, drugs and other contraband into prisons. Across the U.S. and Mexican border, drug smuggling with drones has been detected since 2010. These examples are only a few of the most striking ones. While the usage of the UAVs increases the criminal use of the UAVs will increase too. This increases also causes the need for digital forensics investigation of UAVs.

2.2.2 Digital Forensics Investigation Framework

Carrier and Spafford (2004), presents a framework for digital forensic that includes an investigation process model based on "physical crime scene procedures", at "The Digital Forensic Research Conference DFRWS-2004". They indicate that objective of

an investigation is to "reconstruct the events by using evidence so that hypotheses can be developed and tested".

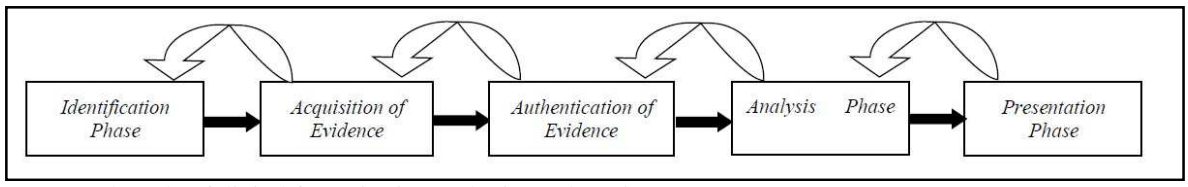
The term *Forensic Investigation* is defined as a "process that uses science and technology to develop and test theories, which can be entered into a court of law, to answer questions about events that occurred". The paper also defines the common digital analysis types: "Media analysis, media management analysis, file system analysis, application analysis, network analysis, OS analysis, executable analysis, image analysis and video analysis".

Ieong (2006), presents FORZA: "Digital Forensics Investigation Framework That Incorporate Legal Issues" at "The Digital Forensic Research Conference DFRWS-2006". In the paper, the fundamental principle of digital forensics investigation was highlighted, which are "Reconnaissance, Reliability and Relevancy". Besides the paper reveals six key questions: "What (the data attributes), Why (the motivation), How (the procedures), Who (the people), Where (the location) and When (the time)".

Harbawi and Varol (2016), investigate the most commonly used tools for digital forensic investigation and gives brief information about these tools. Also in the study, the main principles and concept of the subject are mentioned.

According to the paper Digital Forensic Investigation has five main steps which are shown in Figure 2.2:

Figure 2.2: Digital Forensics Investigation Process



Source: The role of digital forensics in combating cybercrimes.

i. Identification: Before starting any investigation process, all the relevant physical and digital elements should be identified. (computers, mobile phones, PDAs, tablets, or any other electronic device may contain and store digital information, and storage devices such as hard disks, pen drives, CDs, DVDs and other peripheral device capable of storing digital data.)

ii. Acquisition: All the data found on the identified items should be copied forensically.

iii. Preservation: In this step, It must be taken into consideration that the data on the evidence should not be altered while copying process. The investigation process should be applied to the best working copy of the evidence image.

iv. Examining and analyzing: Digital evidence should be categorized to find the best analyzing tools and techniques and proper analyzing techniques should be applied to this evidence.

v. Presentation: All of the findings should be reported with understandable language.

2.2.3 Reverse Engineering For Forensics Investigation

Li and Chen (2011), investigate automatic reverse engineering tools on the basis of methods and their achievements. In the paper, they emphasize the importance of deriving the syntaxes of unknown protocols, in terms of security aspects. Also, they identified the targets and obstacles in automatic protocol reverse engineering.

They investigate the protocol reverse engineering in four different methods as "Manual Work", "Network-based Methods", "Program-based Methods" and "Hybrid Methods". Afterward, they examined the most popular automatic reverse engineering tools and

give some brief information about these tools. The tools mentioned in the paper and used reverse engineering methods in these are: PI (Network-based), ScriptGen (Network-based), Role Player (Network-based), Discoverer (Network-based), Polyglot (Hybrid), AutoFormat(Hybrid), Prospex (Hybrid), Reformat (Hybrid), Rewards (Program-based).

2.2.4 Image File Headers

Alvarez (2004), reveals the importance of the "Exchangeable Image File (EXIF)" in accordance with digital evidence analysis. According to the article, some valuable information can be acquired by reviewing of metadata of the pictures, namely EXIF data. The format and the contained information in EXIF header changes according to the manufacturer and the properties of the camera.

Generally, EXIF header contains manufacturer and the model of the camera, file creation date and time, the date and the time of the picture taken, some properties of the camera while the picture was taken such as focal length, aperture, exposure time, file name and file size. Even some cameras contain GPS position data in EXIF header. The date and the time of the picture taken will not change, in case of moving to another device. If the picture modified by any picture processing tools such as Photoshop or Paint the EXIF header also changes. For this reason, the investigator can identify that if the image has processed any modification or not.

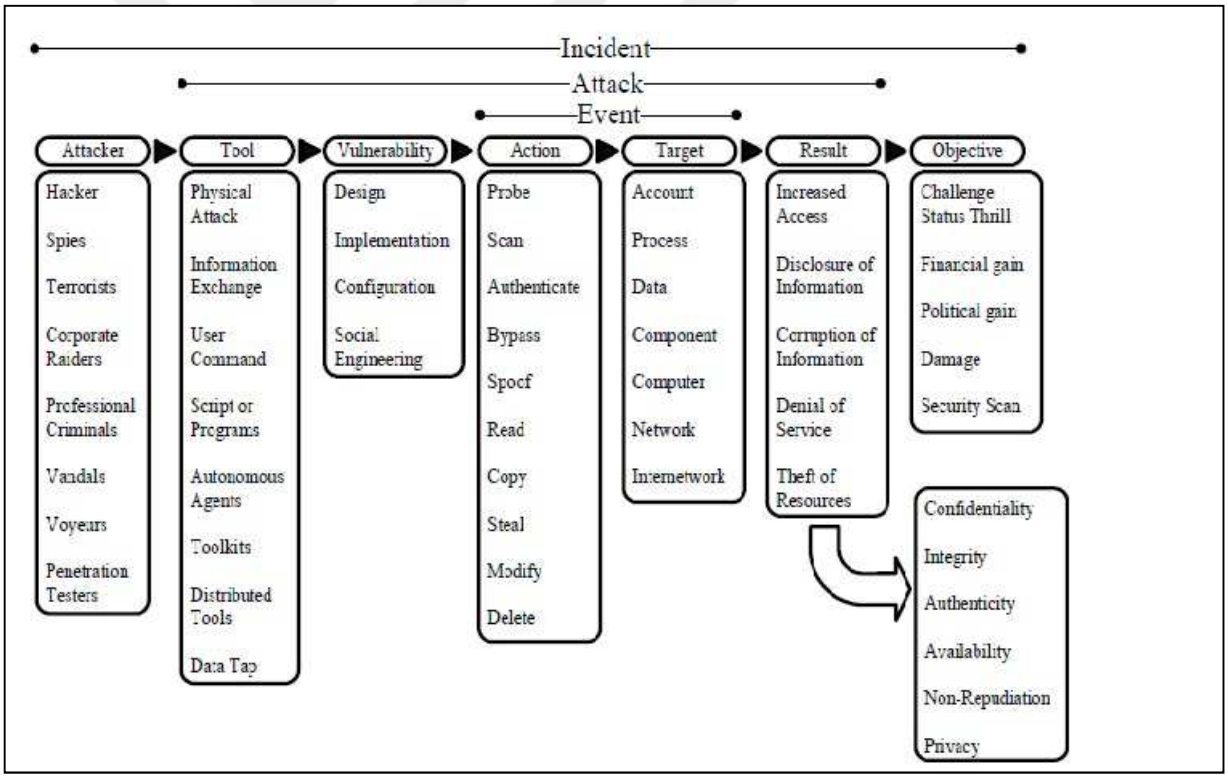
2.2.5 UAV's Digital Forensic Investigation

Bristeau and others (2011), aim to present the "control technology embedded inside the Parrot Ar.Drone". The paper reveals the hardware and running algorithms on the drone. The Parrot Ar.Drone has a main board embedded with a "Parrot P6 processor(32bits ARM9-core, running at 468 MHz), Navigation Board embedded with PIC microcontroller (16 bits, 40 MHZ), a Wi-Fi chip, Camera, Ultrasonic Sensors, Accelerometers, Gyroscopes and a GPS chip".

The P6 processor runs a "Linux based real-time operating system" and all the calculation software packages. The operating system manages "Wi-Fi communication, video data sapling, video compression (for wireless transmission), image processing and sensor acquisitions". Navigation board serves as an interface between sensors (3-axis accelerometers, 2-axis gyroscope, 1-axis vertical gyroscope and ultrasonic sensors).

Samland and others (2012), analyzed the security threads of an s-UAV by using "Computer Emergency Response Team (CERT) taxonomy". The extended CERT taxonomy is showed in Figure 2.3 They examined the components of the 4 popular drones in 2012 and split the components into two categories as hardware and software. Then they reveal the vulnerabilities of these components.

Figure 2.3: The Extended Taxonomy of CERT



Source: Taxonomy for computer security incidents.

In the article, they researched three different scenarios: "Hijacking the Ar.Drone", "Interception of 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 technologies, the UAVs 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 in the market anymore. Therefore, the techniques used in this study is not applicable for the forensic investigation of the currently used UAVs.

Horsman (2016), committed "digital forensic analysis of a Parrot Bebop UAV" which is one of the most popular drones in 2015. Horsman identifies four main processes to implement UAV forensic investigation, which are: "Acquisition of data", "Establishing Flight Data", "Media Taken by the Device" and "Establishing Ownership".

The component investigation of Parrot Bebop is mentioned in the article and some useful properties are identified. The Parrot Bebop UAV seems as a wireless access point and the connection is not password protected. The UAV contains an 8 Gb capacity internal flash memory formatted with "EXT4" file system. The evidential information cannot be accessed with USB connection. Horsman established a wireless network connection and uses "Telnet and File Transfer Protocol(FTP)" to access the hidden folders which contain some evidential information such as Flight Logs.

Kovar (2016, 2015) SANS DFIR 2016 and 2015 presentations focused on the "forensic analysis of both DJI Phantom II and Phantom III". In the presentations, Kovar indicates the artifacts of the UAS. DJI Phantom III contains two flight log files. One of these log files is created by the used mobile devices(smartphones, tablets) and stored in those devices. The other log files are stored in a 4 Gb capacity micro SD card. The micro SD card is on the bottom of the main board of the UAV. These log files cannot be read directly. In the presentation, some online and offline tools to read the files are mentioned.

Clark and others (2017) performed "Digital Forensic Investigation of DJI Phantom III". In their research, they ascertain that DJI Phantom III series UAVs stores 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 files are stored on the UAV's internal nonvolatile storage. The correlate both of these log files and reveal

that these log files are one to one match. In their research, they emphasize both of these log files could be used as evidence in front of the court.

Maarse and Sangers (2016), perform "digital forensic investigation of a DJI Phantom II"; which is an earlier model of "DJI Phantom III". Their study focuses on retrieving positional data and sequence work to build the flight path of the UAV. The research focuses on the flight data, recorded to Ground Control Station, by DJI vision app and EXIF data on the media files.

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

Jain and Others (2017) proposed a UAV Digital Forensic Investigation Framework. 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.

2.2.6 UAV's Vulnerabilities

Baktir and Ogul (2013), remarks the development and increment usage of "cellular networks; Third-Generation (3G) and Long Term Evolution (LTE)". They performed "Denial of Service (DoS)" and flooding attacks on 3G networks and measured their effects.

In the article, They performed "DoS and flooding attacks" in a cellular mobile network that supports 120,000 concurrent users and investigated the effects on the network hardware such as "Radio Network Controller (RNG) and Serving GPRS Support Node (SGSN)". The RNG is used for both data and voice services; hence it is mentioned as one of the most critical equipment in a mobile network. During the attacks CPU on the

RNG is overloaded caused by the high traffic; consequently, the RNG becomes out of service. This situation affects both voice and data subscribers.

Luo (2016), reveals the vulnerabilities of DJI Phantom 3 UAS in Defcon 24 Conference. He classifies the components of the UAV in three categories as "Drone", "Remote Controller" and "Apps/SDKs". The listed items are found to be vulnerable to hijacking.

Drone:

2.4GHz Radio Module,

GPS Module,

Micro USB Port.

Remote Controller:

2.4GHz Radio Module,

USB Port.

Apps/SDKs:

Connect to remote control, display drone information (image of camera, GPS and Compass Data),

Operator Drone (drone takeoff, automatic return).

In the conference, Luo shows hijacking the these listed items and also how to prevent these vulnerabilities. Trujano and others (2016) also perform a similar research to reveal the DJI Phantom III standard vulnerabilities. On their work insecurity of communication links between the UAS components are underlined.

3. DATA AND METHODS

As it is observed in the literature search, a UAV contains lots of artifacts that can be used in the digital forensic analysis. In this section DJI's Phantom III Professional drone will be analyzed in terms of artifacts that is contained by the drone. Besides, there has been no standardized investigation framework for the digital forensic investigation of a UAV at the time of this study. For these reasons as a first step of this study, DJI Phantom III Professional drone will be introduced to get familiar with this flying embedded system. Secondly, a framework for digital forensics investigation of a UAV, proposed and applied to the sample UAS. Then, data acquisition techniques for UAVs will be explained. Lastly, UAV Artifacts will be introduced.

This section covers the DJI Phantom III Professional Drone Review, Investigation Framework Creation, Data Acquisition and Unmanned Aerial Vehicle Artifacts.

3.1 DJI PHANTOM III PROFESSIONAL DRONE REVIEW

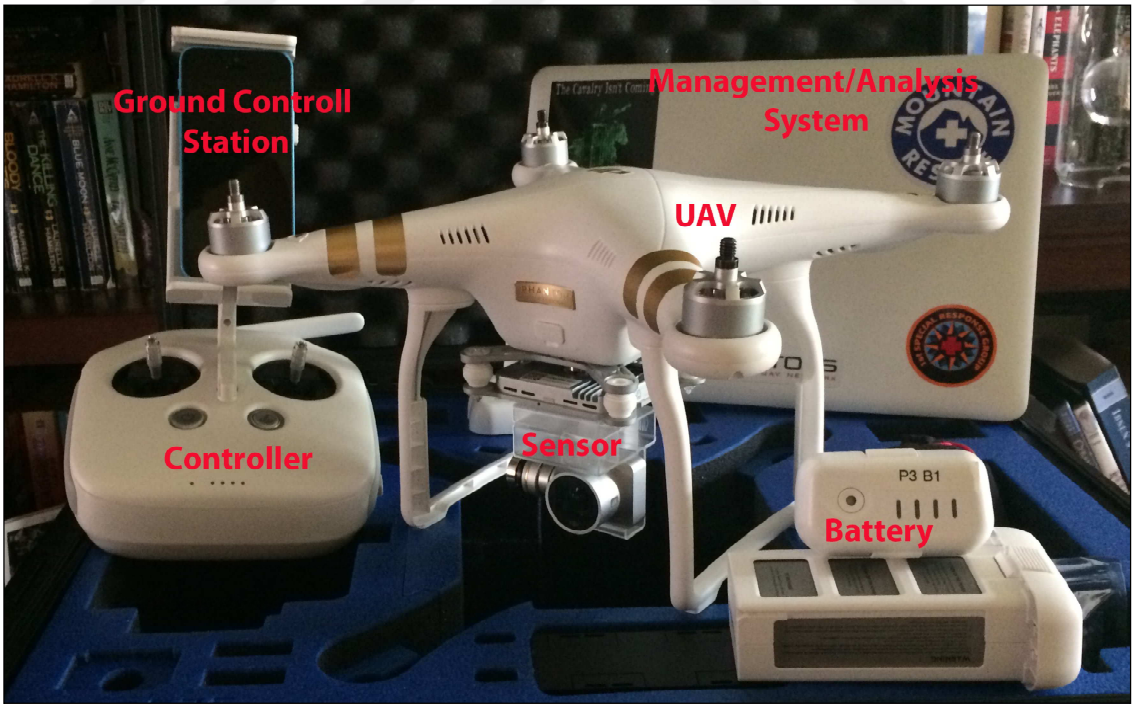
UAVs are introduced as "Flying Embedded Systems". There are wide range of UAVs on the market. The prices of UAVs vary between under a hundred USD to over a few million USD. The prices of a UAV varies according to properties of the UAV. This study aims to investigate the publicly affordable UAVs. The UAVs used for military purposes are out of the scope of this study.

There are numerous kind of commercial drones in the market. Each commercial drone company uses different kind of hardware and software packages. Consequently, different drone company means different systems, different data types and different artifacts. As a result, no single investigation techniques and tools could be used for forensically analysis of a UAV. Besides, there are lots of hobbyist forums about homemade drones. These homemade drones make it more complicated to develop a single UAV investigation tool.

According to the FAA records, DJI is the leader company of the commercial drone business. DJI holds the 70 percent of the drone market. DJI Phantom III models are known as best seller drone in the 2015 and 2016. Besides, DJI Phantom III contains the all major parts of a UAV into a small commercial drone. For these reasons, DJI Phantom III Professional Drone has been chosen as a research item for this study. Moreover, DJI Phantom III already detected on lots of illegal activities for instance, dropping bombs, remote surveillance, plane watching etc. Besides, terrorist groups such as ISIS uses the this drones actively.

On a quick overview of an Unmanned Aerial System (UAS) of DJI Phantom III, the two main observed components are aircraft and ground control station (GCS). While aircraft contains battery, gimbal and camera; ground control station contains remote controller, mobile device and laptop. All of these components has some artifacts for forensic analysis. An example UAS is shown in figure 3.1.

Figure 3.1: An Example Unmanned Aerial System



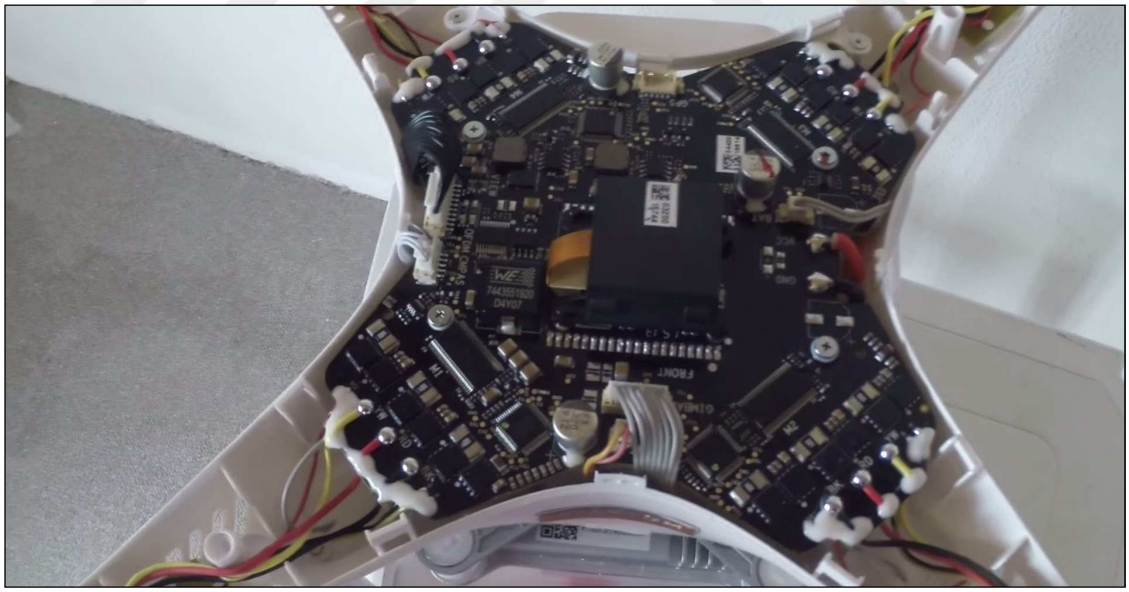
Source: D. Kovar, "UAV (aka drone) Forensics"

a. *Aircraft:* DJI Phantom III aircraft may be seems like a small drone at first glance, but it is one of the most powerful commercial drone on the market. The weight of the

aircraft is 1,280 grams and the diagonal size (propellers excluded) is 350 millimeters. It can reach maximum altitude 19,685 ft (6,000meters) above the sea level which is above some private planes. (such as Cessna Skyhawk's maximum operating altitude is 16,000 ft). It has 16 m/s (approx. 57 km/h) maximum speed. The aircraft contains both GPS and GLONASS systems as satellite positioning system.

Inside the aircraft body, there are four brushless electric motors for propellers and four electronic speed control unit for each motor. The Figure 3.2 shows the interior of the DJI Phantom III. It can be observed that all of the modules contains on a single board. The GPS antenna is glued to the upper side of the drone case and protected with anti RF cover. The main board maintains IMU, gyroscope, speed controller and Wi-Fi modules. Also, there is a 4 GB capacity SD-card in the back of the main board which contains highly detailed flight information. The stored files on this card will be inspected in the following sections.

Figure 3.2: Interior of DJI Phantom III



The aircraft body also contains intelligent flight battery. The aircraft powered by 4480mAh Li-Po(Lithium - Polymer) battery. The battery provides up to 25 minutes flight time. Besides, the aircraft contains gimbal and camera. The gimbal adjusts the horizontal and the vertical axis of the camera for capturing more stabilized image. The

gimbal uses IMU data to adjust the camera angle. DJI Phantom III drone maintains a camera with 4K resolution. There is a micro SD-card slot on the gimbal for storing captured videos and pictures of the camera.

b. "Ground Control Station" (GCS): The "ground control station" contains a remote controller, a mobile device (smartphone or tablet) and laptop for image processing (not necessary). The operating frequency of the controller is 2,400-2483GHz. The controller uses Lightbridge protocol to communicate with aircraft. The Lightbridge protocol was developed by DJI. It is a kind of Wi-Fi broadcast protocol to transmit high resolution video packets and control signals to higher distances.

The remote controller is connected to an Android or IOS device with a USB port. DJI Go application is used for real time video display and some of the control functions of the aircraft. DJI Go application stores highly detailed flight information on a .txt extended file. This file will be inspected in the following sections.

3.2 UAV DIGITAL FORENSICS INVESTIGATION FRAMEWORK

There is no standardized investigation framework for UAV at the time of this study. In order to disclose an evidence related with a case to the court of law and to get approved this evidence by a court of law; investigators should use a standardized investigation framework. There are numerous kind of UAVs on the market. Each company uses different equipment and firmware packages. For this reason, although it is difficult to create a single tool for investigating UAVs, a general investigation framework for all kind of UAVs, is a reasonable solution.

Seven-phased framework for UAV investigation that is proposed on this study, is shown on Table 3.1. The framework applied to the sample UAS (DJI Phantom III Professional). The findings of the investigation are explained in the further sections. The framework phases are explained below.

Table 3.1: Seven-phased UAV Investigation Framework

NO	PHASE
1	Preparation
2	Scene Control
3	Customization Detection
4	Data Acquisition
5	Evidence Authentication
6	Evidence Examination
7	Presentation

3.2.1 Preparation Phase

"An embedded system is a special-purpose computer system designed to perform one or a few dedicated functions, for example, MP3 players, mobile phones, PDA, telemetric system such as car navigation system etc"(Lim and Lee 2008). 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. The investigator has to follow the developments in UAV systems and have knowledge about firmware and hardware of the UAS which breaks into the market. An undue response on the incident scene, could cause irreversible damage on evidence. To avoid to cause any data loss, the investigator should have knowledge about hardware and software properties of the specific UAV. Preparation phase divides into two different stages as hardware investigation and firmware investigation.

i, Hardware Investigation Stage : First of all, the investigator should have knowledge about all of the standard hardware components that belong to the UAS, before the arrival at the incident area.

The sample UAS used for this study (DJI Phantom III Professional) consist of two main components, "aircraft and ground control station". 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. With the inside of the aircraft, there are four brushless motors and four electronic speed control unit for each propeller, a single main board which contains all the modules of Inertial Measure Unit (IMU), gyroscope, GPS, speed controller unit and Wi-Fi. The last but not the 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 basically, consists of a remote controller and a mobile device which runs "DJI Go" application. The mobile device is connected to the remote controller with a USB port and the remote controller communicates with the aircraft via Lightbridge protocol on 2,400-2483GHz frequency.

ii, Firmware Investigation Stage : Different UAS uses different firmware, which means they have different data format. According to analyze the data the investigator should know the firmware of the system. Besides, data overflow of the system is also important for an investigation.

The sample UAS uses, "Open WRT 14.07 Barrier Breaker r2879, 14.07" built for "ar71xx/generic" operating system on both aircraft and remote controller (Voidsec, 2017). This firmware is a Linux based operating system used for embedded systems. Consequently, "OverlayFS, tmpfs, SquashFS, JFFS2, UBIFS, ext2, mini_fo" file systems, could be contained by the UAS. In addition, DJI Go application runs on Android or IOS devices. As the same with the drone's internal SD-card, DJI Go application creates a very detailed flight record and stores it on the mobile device.

3.2.2 Scene Control Phase

All kinds of investigation processes that take place on the incidence scene form the scene control phase of the digital forensic investigation. During this phase, an investigator should take into consideration of any dropped equipment from the UAV during the incidence. Besides, maintaining chain of custody and protection of evidence from altering is crucial in this phase. Moreover, 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.

3.2.3 Customization Detection Phase

UASs are very flexible and customizable embedded devices. There are lots of online sources about UAV customization and to apply this changes into an UAS very little or no electronic knowledge is needed. UASs could be modified to perform to specific missions. The investigator should detect these modifications and present them in the report for the court of law. Some of the detected modifications on the UASs during any illegal action listed as:

a, Range extender usage, for flying in more distance,

b, Battery upgrades, for more flight time,

c, Dropping gear, for smuggling and dropping prohibited items to prisons,

d, Camera upgrades, for surveillance,

e, Autopilot software, for pilotless and critical missions such as flying over military units,

f, Deployment with explosives, for terrorist activities,

g, Gun mounting, for terrorist activities.

3.2.4 Data Acquisition Phase

Data Acquisition Phase is probably the most important phase of an investigation and involves the collection of all data based on approved forensically techniques. In this phase, all volatile and non-volatile data should be acquired for instance, network based data, live response data and removable media evidence, etc. In compliance with the "Avoiding Adding Data" principle of digital forensics (ACPO, n.d.), 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 (Jahankhani, 2010).

The sample UAS used in this study contains three kinds of data that could be presented as evidence to in front of the court. The first type of data is stored on the mobile device which runs the "DJI Go" application. This file is a binary file and has .txt extension. The file contains a very detailed flight record. The second kind of the data is stored on the drone's internal 4Gb capacity SD-card. This one is also a binary file and has .dat extension. The .dat extended file contains much more detailed flight records than a .txt extended file. Lastly, the headers of the image files taken by the UAV's camera contains valuable information for the investigation. These image files are stored on the SD-card of the gimbal. The used data acquisition techniques for gathering data from the sample UAS is explained in detail on the following sections.

3.2.5 Evidence Authentication Phase

Evidence authentication phase is significant for the approval of the collected evidence before the court (Wiles, 2007). 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", should be taken into consideration (SWGDE and IOCE, 2000). Besides all of the investigation process should be performed at "Working Copy" of the "Best Copy" that belongs to the original evidence (Sammons, 2012). The used evidence authentication techniques for the sample UAS is explained in detail on the following sections.

3.2.6 Evidence Examination Phase

In evidence examination phase the investigator, probes into all of the data which is acquired from the UAS. The investigator tries to find an evidence about specific cases. The rebuilding of the flight path of a suspicious flight takes a vital role, in case of presenting any evidence to the court of law. Also, every kind of image files such as pictures or videos could be used as an evidence. The examination techniques used for the data acquired from the sample UAS are explained in the further sections.

3.2.7 Presentation Phase

Lastly but not the least, the presentation phase is the final step of the 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.

3.3 DATA ACQUISITION

The UAS, which is used for this research, consist of DJI Phantom III Professional Drone, DJI Phantom III Professional Remote Controller and an Android tablet (Samsung Galaxy Tab 3 Lite).

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, the factory reset procedures are applied to both the drone and the Samsung Galaxy Tab 3 Lite tablet before performing test flights. The drone was formatted by using DJI Go application. This process removes the all nonvolatile files that is stored on the internal memory of the drone. Then the android tablet formatted to factory settings by using booting menu. After the formatting, the device is updated to the latest android version and the latest version of DJI Go application is installed. As a final precautionary step, the SD card located on the gimbal and used for video and picture storage is wiped by using "Disk Dump (dd) utility (Casey, 2002)" (during the wipe procedure all of the disk is filled by *"00"* with *"zero of"* command) and formatted to FAT32 file system.
Then, ten different flights are planned and conducted. Each of the flights is conducted on different places, in different days and at different times of the days. All of the flights date, time, location and flight pattern information are recorded. The information of the flights are shown on the Table 3.2 Between the flights the Android tablet did not used for any other reasons.

Table 3.2: Flight Information

FLIGHT NUMBER	DATE	TIME INTERVAL	HOME POINT COORDINATES
1	18.07.2017	12:08 - 12:30	37°59'37.06"N - 027°07'09.93"E
2	28.07.2017	10:04 - 10:27	37°43'37.30"N - 030°29'32.77"E
3	10.08.2017	14:42 - 15:08	37°51'56.29"N - 030°50'24.97"E
4	20.08.2017	11:27 - 11:50	41°09'40.00"N - 029°38'32.41"E
5	25.08.2017	15:39 - 15:51	40°58'06.84"N - 029°02'10.40"E
6	01.09.2017	18:22 - 18:35	40°57'25.10"N - 029°04'28.48"E
7	08.09.2017	16:18 - 16:39	40°49'30.00"N - 029°16'45.00"E
8	09.09.2017	11:05 - 11:32	40°48'56.71"N - 029°15'45.87"E
9	16.09.2017	17:40 - 18:04	40°49'11.00"N - 029°16'27.60"E
10	23.09.2017	15:32 - 15:57	40°48'17.15"N - 029°16'27.17"E

After conducting the flights, data acquisition phase has been started. During the data acquisition phase, "md5sum" utility used for MD5 hash generation and FTK Imager tool (Carbone, 2014) used for getting the physical image of the Android tablet storage and SD card memory of the UAS. Firstly, the hash of the Android tablet storage is generated and then image of the tablet is generated. The hash values of the "md5sum" utility and FTK Imager tool were compared and verified. The image is labeled as *"Evidence_storage_001"* (Hoog and McCash, 2011). Secondly, hash of the drone's storage equipment is generated and then imaged. Again the hash values of both tools were compared and verified. The image is labeled as *"Evidence_storage_002"*. Lastly, the same process applied to the SD card stored on the gimbal and the hash values are compared and verified. The image is labeled as *"Evidence_storage_003"*. All of the images are copied and the investigations are conducted on a best working copy of the images, because during the research the android tablet and drone could be used for other reasons. The evidence authentication data are shown on the Table 3.3.

Table 3.3: Evidence Authentication Data

EVIDENCE	EVIDENCE MD5 HASH (with FTK Imager Tool)	IMAGE OF THE EVIDENCE MD5 HASH (with md5sum tool)
Evidence_storage_001	702aefc3bc17a7ae 0ae983021d3e0685	702aefc3bc17a7ae 0ae983021d3e0685
Evidence_storage_002	1309901b969b1bf7 898c9c1711fb2fd0	1309901b969b1bf7 898c9c1711fb2fd0
Evidence_storage_003	f5d18bd470399ac5 12392ef0771be315	f5d18bd470399ac5 12392ef0771be315

3.4 UNMANNED AERIAL VEHICLE ARTIFACTS

The artifacts that may be contained by a UAV, could be analyzed in two groups such as "Physical" and "Digital" evidence. "Physical evidence" contains, drone, flight controllers, some sensors related with drones, ground control stations, etc. Due to this Physical evidence are in scope of other criminal discipline's examination subject, Physical evidence is out of the scope of this study. Besides, "Digital evidence" contains; mobile operating systems (Android or IOS), some file systems, media storage, data link, etc.

During the literature search, It is found out that DJI Phantom III UAS keep records of the each flight in two different files. Normally, these flight logs are used by DJI such reasons like; maintenance, fault detection and crash analysis. These Flight Logs can be used for Digital Forensic Investigation of a UAV, for this reason, the study is focused on these two files.

As a consequence of this research three digital evidences are located. First of these evidence is a ".TXT" extended file and created by "DJI Go" application. This TXT file stored on the smart device which is used for controlling the drone. The second evidence is a ".DAT" extended file and created by the drone itself. This file is stored on the drone's internal memory. Lastly, the third evidence is the EXIF data of the pictures taken by the camera of the drone.

3.4.1 DJI Go .TXT File

During the investigation of the Android tablet image, several directories are detected pertain to DJI. The investigation on the smart device is mainly focused on these directories. On the *data/dji.pilot/DJI/FlightRecords* directory, the file named as *DJIFlightRecordyYYYY-MM-DD_[HH-MM-SS].txt* takes attention. This text file cannot be opened by any text editor, even though some online tools convert this file to a readable .csv file.[3]

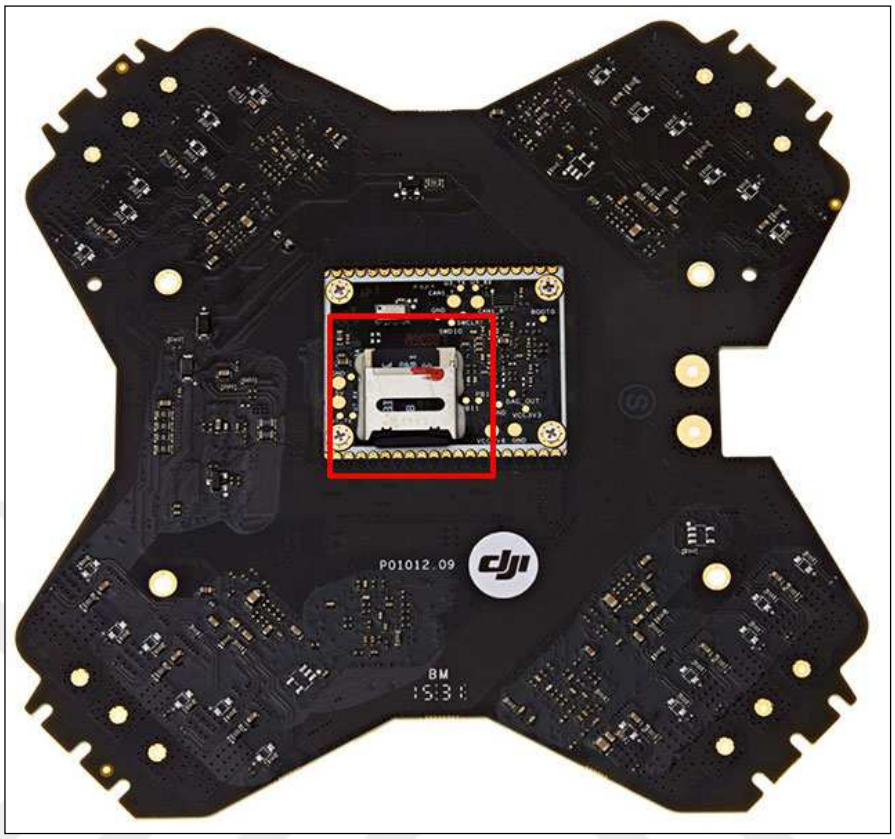
When the data is converted to a .csv file, it is certain that this file is the black box of the drone on the smart device. None of the tools that are used for converting this flight records are a forensically examination tools so that; one of the targets of this research is to ascertain the structure of the file.

3.4.2 .DAT File Created by DJI Drone

DJI Phantom III drones contains a 4 Gb capacity micro SD-Card on the bottom of the mainboard. Figure 3.3 shows the location of the SD-Card. To access this storage hardware, the aircraft has to be laid open and the mainboard must be removed from the aircraft. The SD-Card is glued to the card slot and the glue should be scratched to remove the SD-Card. The SD-Card imaged and the image was labeled as *"Evidence_Storage_002"*. To prevent any data loss, the Evidence_Storage_002 is copied. This copy was inspected with scrutiny. During the inspection, 10 files, named as FLY***.DAT were detected. The numbers *** in the file names were consecutive numbers. It is detected that these .dat extended files are in binary format.

[3] https://airdata.com/

Figure 3.3: DJI Phantom III Internal SD-Card



At first glance, that is detected that the files are encoded. Even though there is quite a little official information about these files, some hobbyists were worked hard to decode the files. Even some of them created their own tools. A tool called Datcon[4] is the one of the most prospering ones. Datcon converts these files to a readable .csv file, however, this tool cannot convert all of the data.

3.4.3 EXIF Data

DJI Phantom III drones store all of the media recorded videos and taken pictures in an SD-Card stored in the gimbal. In the way that other storage equipment of the drone, this SD-Card was imaged and the image was labeled as "*Evidence_Storage_003*".

[4] https://datfile.net/

A few pictures are exported from the image to analyze the metadata of the pictures. At first glance, the drone stores the pictures as .jpg extended files and videos as .mov extended files. The EXIF headers of the image were read with a tool called "ExifTool"[5] it is detected that it has lots of valuable information for an investigation such as the creation date and GPS position. An example EXIF data is shown on appendix1**.**

[5] https://www.sno.phy.queensu.ca/~phil/exiftool/

4. FINDINGS

In this section, UAS artifacts which are specified in the previous section, are investigated throughly. As a consequence of the flight records are stored on the binary files and cannot readable throughly, data structures of the flight records are put in the effort to find out. The binary files are observed by every detail to find evidence. In this observation, binary analysis, reverse engineering and decryption algorithms are considered.

This section presents the findings by the analyzing data that is acquired from the UAS. This section covers .dat file data structure, .txt file data structure, EXIF header data structure and tool creation.

4.1 .DAT FILE DATA STRUCTURE

As it is mentioned in the previous sections, one of the artifacts, that our sample UAS contains, is a .dat extended binary file. This file is located on the nonvolatile internal memory of the aircraft and to acquire this storage equipment, the aircraft must be laid open and the mainboard has to be removed from the aircraft.

"Evidence_storage_002" investigated throughly to find any substantial data to present court of law about any incident. It is found out that the aircraft creates a new .dat extended file on every startup. The size of this file depends on the running time of the UAS. For instance, a file named "FLY001.dat", with the size of 1.760 KB, was created in our tests. This file corresponds to the operation of 10 seconds of turning on the drone without a takeoff. Likewise, another file, named "FLY009.dat", with the size of 275.104 KB, was created which belonged to an approximately 25 minute flight operation.

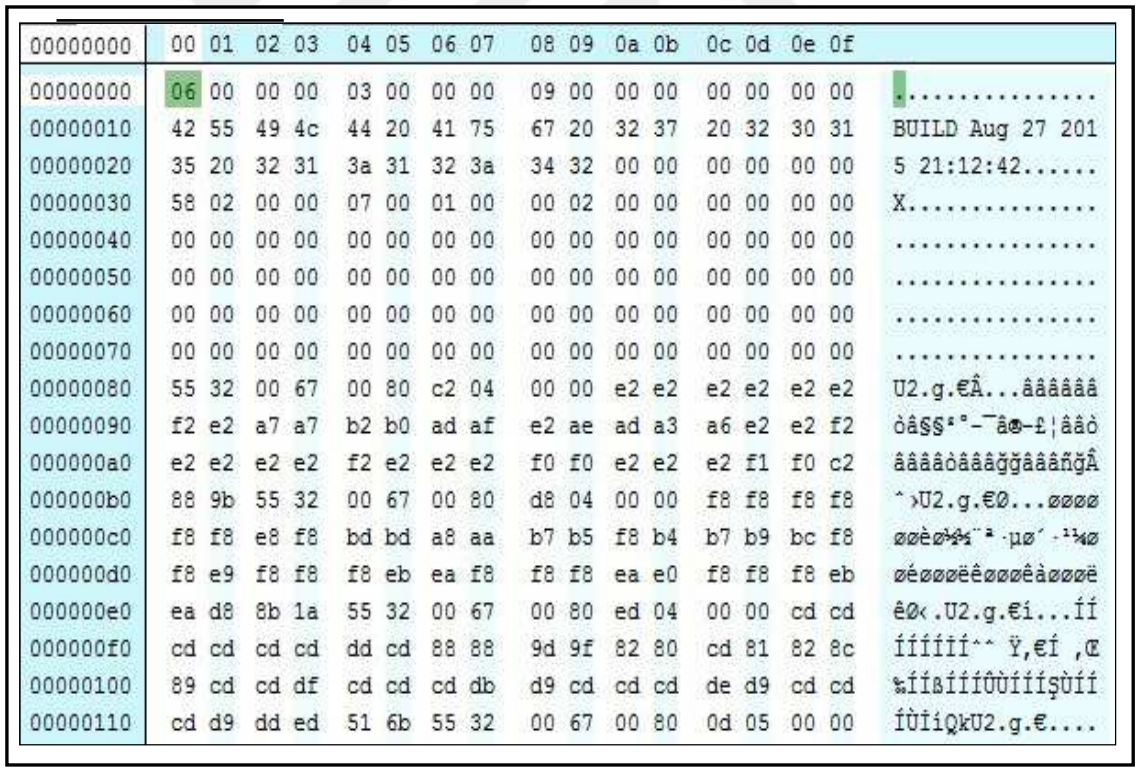
After the drone's internal nonvolatile storage equipment imaged, some preliminary investigation is conducted to read the files. As the first observations of the evidence

detected as; the drone's internal nonvolatile memory has FAT32 file system. Besides the files are in binary format and encoded.

There is very limited official information about the content of the .dat extended files created and stored in the UAV. Nevertheless, in the hobbyist's community, there are lots of discussion about the flight records of the DJI. Some hobbyists created tools the decode the .dat extended files, however, none of them are forensically investigation tools and these tools cannot decode the all of the files.

Since the .dat extended flight records are stored in binary formatted files, we focused on retrieving the data structure of the file by using a binary editor tool. The Figure 4.1 shows the screenshot of a .dat file as it is seen on a binary editor tool.

Figure 4.1: Screenshot of a .Dat File on a Binary Editor Tool

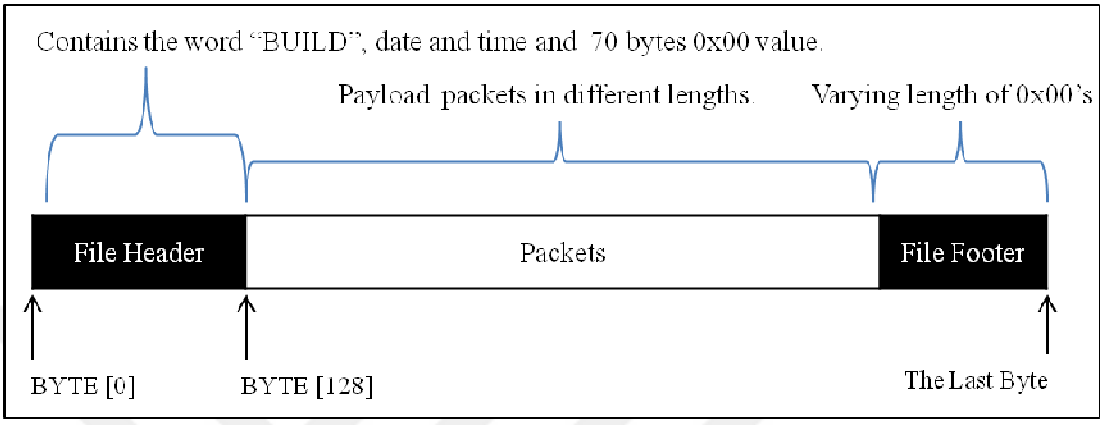


00000000	00 01 02 03	04 05 06 07	08 09 0a 0b	0c 0d 0e 0f	
00000000	06 00 00 00	03 00 00 00	09 00 00 00	00 00 00 00	.....
00000010	42 55 49 4c	44 20 41 75	67 20 32 37	20 32 30 31	BUILD Aug 27 201
00000020	35 20 32 31	3a 31 32 3a	34 32 00 00	00 00 00 00	5 21:12:42.....
00000030	58 02 00 00	07 00 01 00	00 02 00 00	00 00 00 00	X.....
00000040	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000050	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000060	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000070	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000080	55 32 00 67	00 80 c2 04	00 00 e2 e2	e2 e2 e2 e2	U2.g.€Â...ââââââ
00000090	f2 e2 a7 a7	b2 b0 ad af	e2 ae ad a3	a6 e2 e2 f2	òâ§§²°-¯â®-£¦ââò
000000a0	e2 e2 e2 e2	f2 e2 e2 e2	f0 f0 e2 e2	e2 f1 f0 c2	ââââòâââğğâââñğÂ
000000b0	88 9b 55 32	00 67 00 80	d8 04 00 00	f8 f8 f8 f8	ˆ›U2.g.€Ø...øøøø
000000c0	f8 f8 e8 f8	bd bd a8 aa	b7 b5 f8 b4	b7 b9 bc f8	øøèø½½¨ª·µø´·¹¼ø
000000d0	f8 e9 f8 f8	f8 eb ea f8	f8 f8 ea e0	f8 f8 f8 eb	øéøøøëêøøøêàøøøë
000000e0	ea d8 8b 1a	55 32 00 67	00 80 ed 04	00 00 cd cd	êØ‹.U2.g.€í...ÍÍ
000000f0	cd cd cd cd	dd cd 88 88	9d 9f 82 80	cd 81 82 8c	ÍÍÍÍÝÍˆˆ Ÿ‚€Í ‚Œ
00000100	89 cd cd df	cd cd cd db	d9 cd cd cd	de d9 cd cd	‰ÍÍßÍÍÍÛÙÍÍÍŞÙÍÍ
00000110	cd d9 dd ed	51 6b 55 32	00 67 00 80	0d 05 00 00	ÍÙÝíQkU2.g.€....

As it is seen on the Figure 4.1 first 128 bytes of the .dat file is file header. Each .dat file contains the word "BUILD" in 16-20 bytes. Then a followed by a date and time. There are no exact information about what does this build date and time refers to. After this

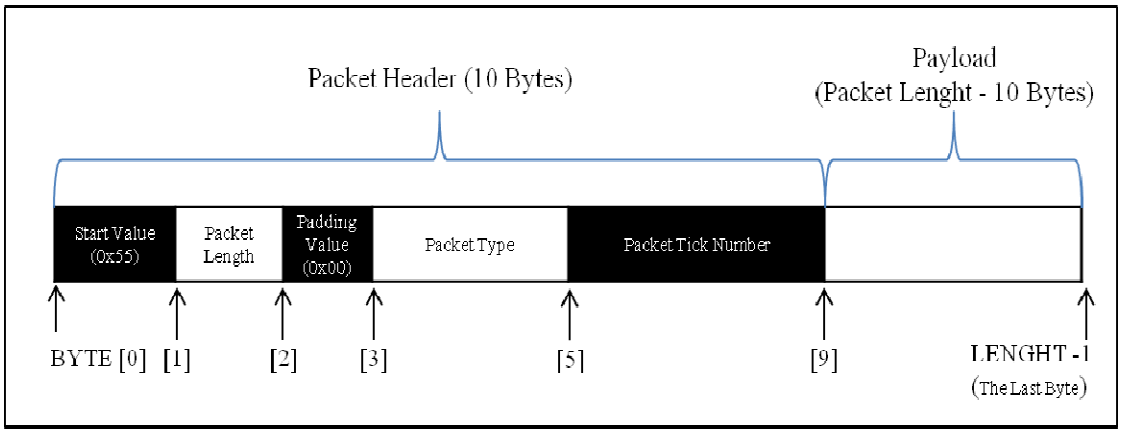
build date and time, file has 00 values until the 128th of the bytes where the actual payloads starting. Figure 4.2 shows the general overview of the file structure. The .Dat file ends with 0x00 values of varying numbers of bytes.

Figure 4.2: General Overview A .dat Extended Flight Record File



The length of each data packet varies depending on the type of data packet that is written. Even though the lengths of data packets vary, all packets have a common structure. The first 10 bytes of each data packet is packet header. Each packet starts with 0x55 value on its first byte. After the start byte packet length (in bytes) is assigned to the next one byte. This packet length shows the whole packet length and contains the start byte and the last byte of the whole packet. After this packet length information, the next byte is always filled with padding value of 0x00. After the padding, the byte[3, 4] shows the packet type. Byte [5:9] is the packet tick number. Figure 4.3 shows the general overview of the packet structure.

Figure 4.3: General Overview Of The Packet Structure Of A .dat Extended File



We are able to locate 9 data packet types in the .dat extended file. These packet types are "GPS, Motor, Home Point, Remote Control, Tablet Location, Battery, Gimbal, Flight Status and Advanced Battery". Table 4.1 presents the packet type values of each packet type.

Table 4.1: . dat Extended Flight Record File Packet Type Values

Packet Type	Value
GPS	0xCF01
Motor	0xDAF1
Gimbal	0x2C34
Flight Status	0x2A0c
Home Point	0xC60D
Tablet Location	0xc12B
Remote Control	0x9800
Battery	0x1E12
Advanced Battery	0x4411

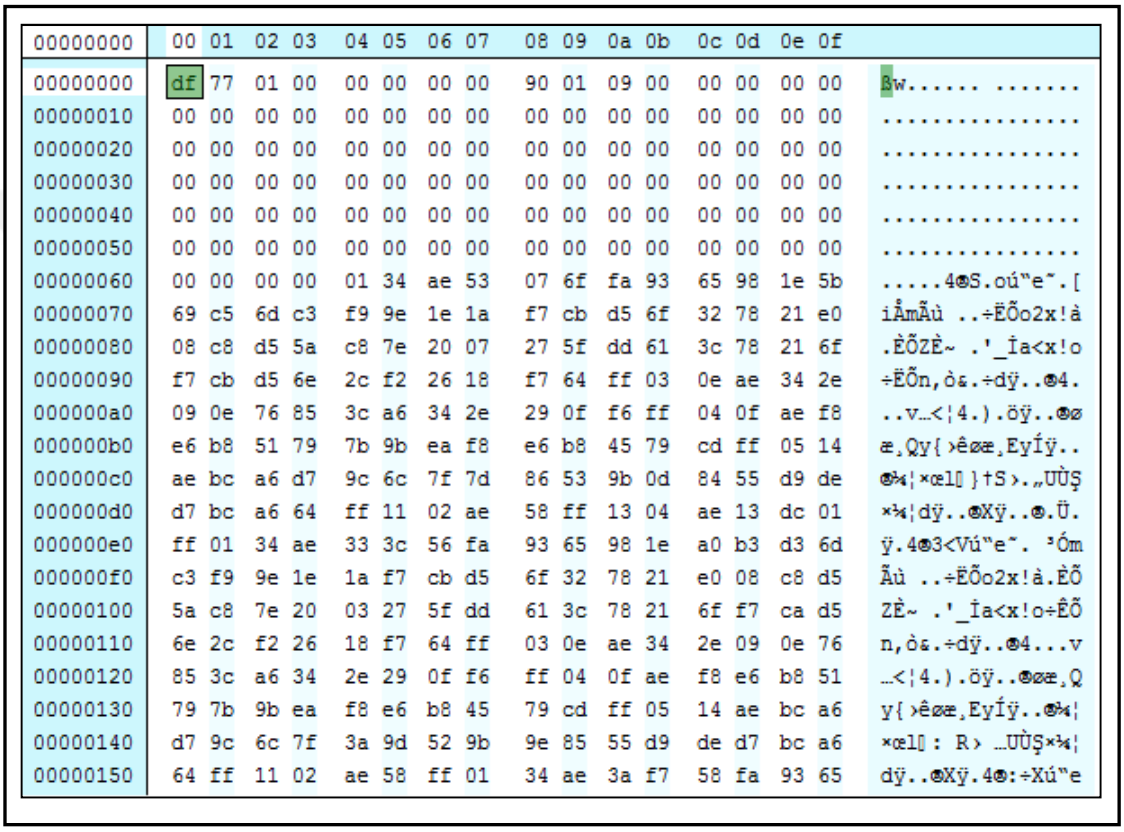
Packet payload structure changes according to the packet type. The full packet structure that contains the payload structure is explained in depth in Appendix 2. In Appendix 2 the payloads and their parts are explained.

4.2 .TXT FILE DATA STRUCTURE

The .txt extended flight record is another artifact that is found in the sample UAS, presented hereinbefore. The .txt extended flight record file is created by an Android application(DJI Go) and it is stored in the nonvolatile memory of the mobile device. These files are stored on the *"/dji.pilot/DJI/FlightRecords"* directory of the mobile device. As a first step, the file was tried to open by a text editor, and it is detected that this file is a binary file.

The data structure of the .dat file was applied to the DJI Go .txt file and it is found out that .txt file has a proprietary format and it is different than the .dat extended file. Then the file is opened by a binary editor. The Figure 4.4 shows the screenshot of a .dat file as it is seen on a binary editor tool. There are only one online tool which converts this .txt files into a human readable .csv file[6].

Figure 4.4: Screenshot of a .Txt File on a Binary Editor Tool



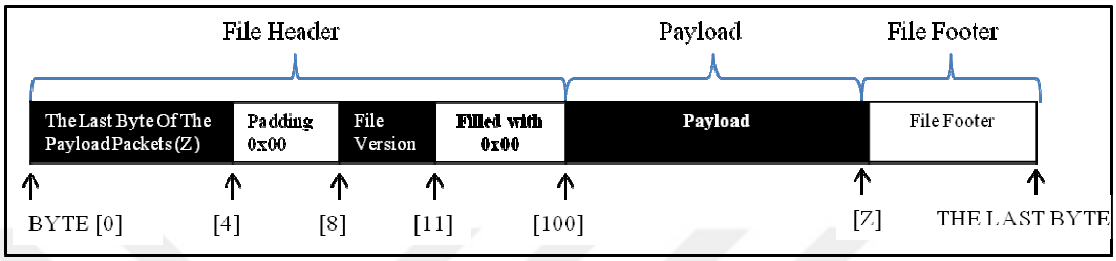
00000000	00 01 02 03	04 05 06 07	08 09 0a 0b	0c 0d 0e 0f	
00000000	df 77 01 00	00 00 00 00	90 01 09 00	00 00 00 00	ßw..... .....
00000010	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000020	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000030	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000040	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000050	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
00000060	00 00 00 00	01 34 ae 53	07 6f fa 93	65 98 1e 5b	.....4®S.oú"e˜.[
00000070	69 c5 6d c3	f9 9e 1e 1a	f7 cb d5 6f	32 78 21 e0	iÅmÃù ..÷ËÕo2x!à
00000080	08 c8 d5 5a	c8 7e 20 07	27 5f dd 61	3c 78 21 6f	.ÈÕZÈ~ .'_Ýa<x!o
00000090	f7 cb d5 6e	2c f2 26 18	f7 64 ff 03	0e ae 34 2e	÷ËÕn,ò&.÷dÿ..®4.
000000a0	09 0e 76 85	3c a6 34 2e	29 0f f6 ff	04 0f ae f8	..v…<¦4.).öÿ..®ø
000000b0	e6 b8 51 79	7b 9b ea f8	e6 b8 45 79	cd ff 05 14	æ¸Qy{›êøæ¸EyÍÿ..
000000c0	ae bc a6 d7	9c 6c 7f 7d	86 53 9b 0d	84 55 d9 de	®¾¦×œl}†S›.„UÙŞ
000000d0	d7 bc a6 64	ff 11 02 ae	58 ff 13 04	ae 13 dc 01	×¾¦dÿ..®Xÿ..®.Ü.
000000e0	ff 01 34 ae	33 3c 56 fa	93 65 98 1e	a0 b3 d3 6d	ÿ.4®3<Vú"e˜. ³Óm
000000f0	c3 f9 9e 1e	1a f7 cb d5	6f 32 78 21	e0 08 c8 d5	Ãù ..÷ËÕo2x!à.ÈÕ
00000100	5a c8 7e 20	03 27 5f dd	61 3c 78 21	6f f7 ca d5	ZÈ~ .'_Ýa<x!o÷ÊÕ
00000110	6e 2c f2 26	18 f7 64 ff	03 0e ae 34	2e 09 0e 76	n,ò&.÷dÿ..®4...v
00000120	85 3c a6 34	2e 29 0f f6	ff 04 0f ae	f8 e6 b8 51	…<¦4.).öÿ..®øæ¸Q
00000130	79 7b 9b ea	f8 e6 b8 45	79 cd ff 05	14 ae bc a6	y{›êøæ¸EyÍÿ..®¾¦
00000140	d7 9c 6c 7f	3a 9d 52 9b	9e 85 55 d9	de d7 bc a6	×œl: R› …UÙŞ×¾¦
00000150	64 ff 11 02	ae 58 ff 01	34 ae 3a f7	58 fa 93 65	dÿ..®Xÿ.4®:÷Xú"e

The .txt file was inspected manually. It is detected that the file has little endian encoding. During the inspection several .txt file was opened by binary editor, besides these .txt files are converted to human readable .csv files via the online tool and the .csv versions of the files used during the manual inspection. During the inspection general structure of the file was revealed. The first 100 bytes of the file is file header. In the file header first four bytes shows the last byte of the payload packets which is 0xFF. Then the next four bytes is filled with 0x00. Next three bytes represent the file version. The bytes [11:99] are filled with 0x00. After the file header bytes, the payload section

[6] https://airdata.com/

begins. After the last byte of the payload packages which is 0xFF value, the file footer comes. The length of the footer changes in every file. The file footer contains some valuable information about the drone. Figure 4.5 shows the general overview of the .txt extended flight record file structure.

Figure 4.5: General Overview of the .Txt File Structure



The entropy of the payload is calculated to find out any encryption occurrence. Entropy value of the payload is 7.80. This value shows that the payload is encrypted (Conte and Wolfe 2014). As it is mentioned earlier .txt file is created by DJI Go application. Therefore DJI Go application tried to reverse engineer to reveal the file structure and encryption algorithm. The latest version of the application was downloaded[7] and decompiled. Even though most of the variables, functions and class names are bewildered; "k.class" in the "dji.pilot.fpv.model package of class3.jar" was being used for handling the writing process of flight records. Some of the packet type values are located. The located packet type values are shown on Table 4.2.

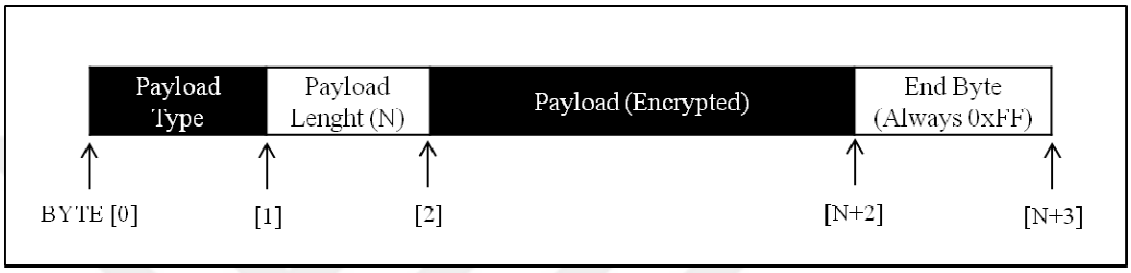
Table 4.2: .txt Extended Flight Record File Packet Type Values

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

[7] https://apkpure.com/dji-go-for-products-before-p4/dji.pilot

The packet structure of the flight records is also revealed by reverse engineering the "DJI Go" application. The packet structure of the flight records shown on the Figure 4.6. Additionally, "libFREncrypt.so" library is located on the "DJIPilot/lib/armeabi-v7a/libFREncrypt.so". This library is detected to used for encryption and decryption of the flight records. No official information is found about this native android library so the payload of the data packets could not be decrypted.

Figure 4.6: General Overview of the .Txt File Packet Structure



Lastly, the file footer comes after the last byte of the payload. As it is mentioned hereinbefore, the last byte of the payload packets are shown on the first four bytes of the file. The file footer length varies in each file. The file footer contains some specific information about the drone in plaintext. In the file footer, flight area and screenshot of the home point is recorded. Besides the name and model of the drone along with the serial numbers of the "Inertial Measure Unit (IMU)", camera, mainboard of the remote control and battery. This information is very crucial in terms of to prove that the flight record belongs to a specific drone.

4.3 EXIF HEADER DATA STRUCTURE

Exchangeable Image File Format (EXIF) header of the images which is taken by UAV's onboard camera, contains lots of valuable information, in terms of the digital forensic investigation. There are lots of tools which extracts the EXIF metadata from the images. An example EXIF data of an image that is taken by the sample UAS is shown on Appendix-1. In the EXIF data of the images that captured with the camera of the sample UAS, location, altitude, creation time and modification times are important information for an investigation.

The byte order of an EXIF header data structure starts with 0xFFD8. Every JPEG file starts with this value and ends with 0xFFD9. The next two bytes after the start value is the metadata version and for the images of the sample UAS, this values is FFE1. Next four bytes shows the length of the EXIF header. EXIF uses TIFF format to store data. According to TIFF format, image information, EXIF information, GPS information, maker notes, interoperability specifications and thumbnail image is stored.

4.4 TOOL CREATION

Since .txt files could not be decrypted properly, a tool created to dissect .dat files for acquiring evidence about a specific crime. "Dat2Csv" is created with Python 3.6 and during the tool creation. During the tool creation, reverse engineering experiments of another offline tool "DatCon", which converts .dat files into human readable .csv files, are applied.

Dat2Csv tool could open .dat files of DJI's all Phantom III, Phantom IV, Mavic and Inspire series. When a .dat file is uploaded to Dat2Csv, the too reads the file in binary format. Then file header is examined to determine the file is a proper flight record or not. To classify the file is proper or not, Dat2Csv checks the bytes between 16 and 20. These bytes should contain the word "BUILD". If the tool detects the word "BUILD", then jumps to byte 128 to read the payloads. If the tool cannot detect the word "BUILD", then throws an exception and exits.

After the file is classified as a proper flight record, the tool starts to read byte 128. According to the packet structure of .dat file hereinbefore and Figure 4.3, each packet starts with 0x55. If Dat2Csv cannot read 0x55 value on the start of each packet, "UnknownPacket" counter is incremented. If the tool reads the starting value, then jumps the next byte to record the packet length. After that, a new "packet" instance is created. Inside the packet instance, packet type, packet tick number and payload are recorded. According to the packet type values which are mentioned on Table 4.1, payload type is detected.

Payloads are encrypted with a weak algorithm. Decryption algorithm of the payload is derived through the reverse engineering experiments of "DatCon". The decryption algorithm uses packet tick number as a key for "XOR" operation. Modulus-256 of the packet tick number calculated to get fix on the length of the key. The decrypted payload is derived by XOR operation of payload and modulus-256 of packet tick number. Figure 4.7 shows the pseudo code of the payload decryption algorithm.

Figure 4.7: Pseudo Code of The Payload Decryption Algorithm

```
def  decrypt_payload (payload, packet_tick_number)
     key = packet_tick_number % 256
     decrypted_payload = [ ]
     for byte in payload
          decrypted_payload.append (byte XOR key)
     return decrypted_payload
```

As mentioned before, packet structure differs according to payload type. Appendix 2 shows the whole packet structure. According to packet structure hereinbefore, payload values are recorded. It is detected that some packets have the same packet tick number value, which means that packets that have the same packet tick numbers are recorded to the .dat file at the same time. Figure 4.8 shows the pseudo code of the Dat2Csv tool.

Figure 4.8: Pseudo Code of The Dat2Csv Tool

```
def Dat2Csv()
    input_file = read .dat file in binary mode
    file_header = bytes 0 to 127 of input_file
    file_check = bytes [16:21] in file_header to string
    if file_check  != "BUILD"
        exit ()
    message = input_file[128:last_byte]
    outfile.open()
    for byte < message.length
        for byte_packet < packet.length
            if byte_packet != 0x55
                Unknown_packet_counter +1
            packet_length = packet [byte_packet+1]
            packet_tick_no = packet [5:9]
            payload = packet [10:packet_length]
        decrypted_payload = decrypt_payload (payload, packet_tick_number)
        payload_data = get_payload_data (decrypted_payload)
        outfile.write(payload_data)
    outfile.close()
    return
```

5. CONCLUSION AND RECOMMENDATIONS

This research aimed to find solutions for detecting and classifying any criminal actions conducted with UAVs. The massive increase in usage of UAVs leads to huge increase in illegal usage. This increase in illegal usage of UAVs, reveals the legal loophole in the aviation regulations and lack of information about investigation techniques about incidents.

Considering that UAVs are also embedded systems, this research started with the idea of digital forensics investigation techniques that are used for other embedded systems could also be applied to UAVs. At the end of the investigation, finding evidence about any suspicious incident for presenting on the court of law is aimed.

At the beginning of the research embedded devices, digital forensics investigation techniques, and related works with the UAVs are reviewed. The studies of Horsman (2015), Kovar (2016,2015) and Maarse and Sangers (2016) are the most relative studies to this research. In their studies, while Horsman analyzed Parrot Bebop UAVs, the others chose DJI Phantom II which is an earlier model of Phantom III. Kovar and Maarse and Sangers mentioned about the flight records of the UAV. Also, in his research Kovar, enlighten the tools which can read the flight records of DJI's UAVs. However, none of the studies involve the data structure of the flight records.

Jain and Others (2017) work was the only one which proposes a standardized investigation framework. They offered a twelve linear phased framework to investigate UAVs. Their investigation phases generally rely on examining the hardware components of the UAV. However, this study proposes a more flexible seven-phased UAV forensic investigation framework which is independent of hardware.

The proposed seven-phased framework applied to the sample UAS. Before the application of the framework, ten different flights are conducted with the UAV. At the end of the investigation, information about the whole flight is acquired; for instance,

whole flight path, altitude, remote control commands, camera and gimbal status, creation date and time of images, image positions, etc. It is experienced that the framework works successfully and significantly helps with the forensic investigation of UASs in a systematic manner.

Three different files; which contains information about flights, found on the sample UAS. One of these files is located on the UAV's internal nonvolatile storage. According to getting the image of this nonvolatile storage, UAV must be unsealed. The other file is flight record which is created by an Android application(DJI Go) and stored in the nonvolatile memory of the mobile device. The last one is metadata information of the images taken by UAV's camera. The EXIF header of the images contains, creation/modification date and time, along with position and altitude information.

Reverse engineering techniques are used to find out file structures of flight records. For this purpose, "DatCon" and Android application "DJI Go" decompiled. File structure and simple decryption algorithm of the .dat extended flight records which is located on the internal nonvolatile memory of the aircraft is completely revealed. The file structure of .txt extended flight records, which is created by DJI Go application and stored on the nonvolatile memory of the Android device, are also revealed. The payload of the file is encrypted and "libFREncrypt.so" library is found to be used on the encryption. However, the encryption of these files could not be cleared up.

"Dat2Csv" tool is created to convert .dat extended flight records into human readable .csv files. Results of the Dat2Csv tool help to create the whole flight path. Also, this tool provides lots of valuable information about flights. The results of "Dat2Csv" tool, could help to find answers and evidence about any incidents that happen during to flight.

UASs are improving with a great momentum, as other fields of the technology. A UAV digital forensics investigator should follow the developments in this field. Each UAV manufacturer uses different hardware and software packages. An undue response on the incident scene could cause irreversible damage on evidence. To avoid to cause

any data loss, the investigator should have knowledge about hardware and software properties of the specific UAV.

There are a few academic researches with concerning about digital forensic investigation of UAVs. As UAVs keep continue to develop rapidly, it will be necessary to create a standardized investigation framework and tools. In this research, only DJI Phantom series drones are investigated. A similar investigation should be conducted to all UAVs on the commercial market. Dat2Csv tool could convert only .dat extended flight records only. As a future work, encryption algorithm of the .txt extended flight log should be cleared up. Lastly, the Dat2Csv tool can convert only DJI's flight logs. A tool which covers the flight logs of the all UAV's on the commercial market should be created.

REFERENCES

Books

Carbone, F., 2014. *Computer forensics with FTK,* Birmingham. U.K.: Packt Publishing.

Casey, E., 2002. *Handbook of computer crime investigation : forensic tools and technology.* San Diego, Calif: Academic Press.

Hoog, A. and McCash, J., 2011. *Android forensics : investigation, analysis and mobile security for google android.* Waltham, MA: Syngress.

Jahankhani, H., 2010. *Handbook of electronic security and digital forensics.* New Jersey: World Scientific.

Sammons, J., 2012. *The basics of digital forensics : the primer for getting started in digital forensics.* Waltham, MA: Syngress, eBook Collection (EBSCOhost).

Valavanis, K. P. and Vachtsevanos, G. J., 2015. *Handbook Of Unmanned Aerial Vehicle (UAV).* Netherlands: Springer.

Wiles, J., 2007. *Technosecurity's guide to e-discovery and digital forensics : a comprehensive handbook.* Burlington, MA: Syngress.

Periodicals

Alvarez, P., 2004. Using extended file information (EXIF) file headers in digital evidence analysis. *International Journal of Digital Evidence*, **2**(3), pp. 1-5.

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, **44**(1), pp. 1477-1484.

Carrier, B., and Spafford, E. H., 2004. An event-based digital forensic investigation framework. *In Digital forensic research workshop* pp. 11-13.

Clarke, R., 2014. Understanding the drone epidemic. *Computer Law & Security Review,* **30**(3), pp. 230-246.

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,* **22**, p. S3-S14, Scopus.

Conte, T. M., & Wolfe, A., 2014. Techniques for detecting encrypted data. *Washington, DC: U.S. Patent and Trademark Office* U.S. Patent No. **8,799,671**.

Cracknell, A. P., 2017. UAVs: regulations and law enforcement. *International Journal of Remote Sensing,* **38**(8-10), pp. 3054-3067, Scopus.

Harbawi, M., and Varol, A., 2016. The role of digital forensics in combating cybercrimes. *In Digital Forensic and Security (ISDFS), 2016 4th International Symposium* pp. 138-142, IEEE. doi:10.1109/ISDFS.2016.7473532.

Hartzler, V., 2018. Terror from the skies: The drones are coming. *Hill,* 29 Jan. pp. 7.

Horsman, G., 2016. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation,* **16**, pp. 1-11.

Ieong, R. S., 2006. FORZA–Digital forensics investigation framework that incorporate legal issues. *Digital Investigation,* **3**, pp. 29-36.

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

Kiltz, S., Lang, A., and Dittmann, J., 2007. Taxonomy for computer security incidents. *Cyber Warfare and Cyber Terrorism,* pp. 412-417.

Li, X., and Chen, L., 2011. A survey on methods of automatic protocol reverse engineering. *In Computational Intelligence and Security (CIS), 2011 Seventh International Conference* pp. 685-689, IEEE.

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

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.*

Oğul, M., and Baktır, S., 2013. Practical attacks on mobile cellular networks and possible countermeasures. Future Internet, 5(4), 474-489.

Ravich, T. M., 2015. Courts in the drone age. *Northern Kentucky Law Review,* **42** (2), pp. 161.

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

Trujano, F., Chan, B., Beams, G., & Rivera, R., 2016. Security Analysis of DJI Phantom 3 Standard. *Massachusetts Institute of Technology*.

Valjarevic, A., and Venter, H. S., 2016. Introduction of concurrent processes into the digital forensic investigation process. *Australian Journal Of Forensic Sciences,* **48**(3), 339-357. doi:10.1080/00450618.2015.1052754.

Other Publications

Association of Chief Police Officers (ACPO), The principles of digital evidence. n.d., http://www.computerforensicsspecialists.co.uk/blog/the-principles-of-digital-evidence [Access Date: 17.11.2017].

Bart, J., 2015. Small drone crashes near white house despite ban against flights in D.C. *USA Today,* [online] 9 October 2015. https://www.usatoday.com/story/news/2015/10/09/drone-crash-white-house-ellipse-us-park-police-federal-aviation-administration/73641812/ [Access Date: 17.11.2017].

Bellamy, W., 2017. US now has 60,000 part 107 drone pilots. *Avionics,* [online] 7 September 2017. http://www.aviationtoday.com/2017/09/07/us-now-60000-part-107-drone-pilots/ [Access Date: 18.01.2018].

Dent, S., 2017. There are over 770,000 registered drone owners in The US. *Engadget*, [online] 28 March 2017. https://www.engadget.com/2017/03/28/there-are-over-770-000-registered-drone-owners-in-the-us/ [Access Date: 18.01.2018].

Divya, J., 2017. Here are the world's largest drone companies and manufacturers to watch and invest in. *Business Insider*, [online] 18 July 2017. http://www.businessinsider.com/top-drone-manufacturers-companies-invest-stocks-2017-07 [Access Date: 16.09.2017].

DJI Company, 2016. DJI Phantom III Professional User Manual

FAA Aerospace Forecasts 2018 - 38. pp. 39 - 45.

Gregg, P., 2018. Drone vs UAV - What is the difference. [online] 24 January 2018. *https://wiki.ezvid.com/m/drone-vs-uav-what-is-the-difference-_2FJYp_SrUkP-* [Access Date: 16.04.2018]. (Internet Sources).

Kovar, D., Dominguez, G., and Murphy, C., 2016. UAV (aka drone) forensics. 7 July 2016. Slides of a talk given at SANS DFIR summit in Austin, TX.

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.

OpenWRT, n.d. [online] https://wiki.openwrt.org/doc/barrier.breaker. [Access Date: 09.12.2017].

Pomerleau, M., 2017.) In drones, ISIS has its own tactical airforce. *Defense News,* [online] 21 September 2017. https://www.defensenews.com/digital-show-dailies/modern-day-marine/2017/09/21/in-drones-isis-has-its-own-tactical-air-force/ [Access Date: 18.02.2018].

Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE), 2000. Digital evidence: Standards and principles. [online] April 2000. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm [Access Date: 25.10.2017].

U.S. Army, 2005. Unmanned aerial system (UAS) roadmap 2005-2030.

U.S. Army, 2010. Eyes Of The Army - U.S. Army Roadmap for UAS 2010-2035

VoidSec, 2017. Hacking the DJI Phantom III. [online] 13 January 2017. https://voidsec.com/hacking-dji-phantom-3/ [Access Date: 18.01.2018].

White M., 2008. *On a Wind and Prayer* [documentary].

Yue, W., 2016. As China's drone market takes off, leader DJI still flies far above the competition. Forbes, [online] 12 May 2016 https://www.forbes.com/sites/ywang/2016/05/12/chinas-flood-of-cheap-flying-cameras-is-little-threat-to-dajiang/#694e401b1869 [Access Date: 16.09.2017].

APPENDICES

Appendix A.1 An Example EXIF Data

Exif Image Size	4000 × 3000	**Interoperability Index**	R98-DCF basic file (sRGB)
Image Description	DCIM\100MEDIA\ DJI_0020.JPG	**Interoperability Version**	0100
Make	DJI	**Exposure Index**	Undef
Camera Model Name	FC300X	**File Source**	Digital Camera
Orientation	Horizontal (Normal)	**Scene Type**	Unknown(0)
Software	v01.23.3414	**Custom Rendered**	Normal
Modify Date	2016:09:01 13:39:46	**Exposure Mode**	Auto
Y Cb Cr Positioning	Centered	**White Balance**	Auto
Exposure Time	1/1142	**Digital Zoom Ratio**	Undef
F Number	2.80	**Focal Length In 35mm**	20 mm
Exposure Program	Program AE	**Scene Capture Type**	Standard
ISO	100	**Gain Control**	None
EXIF Version	0230	**Contrast**	Normal
Date/Time Original	2016:09:01 13:39:46	**Resolution**	72 pixels/inch
Create Date	2016:09:01 13:39:46	**Saturation**	Normal
Components Configuration	-,Cr, Cb, Y	**Sharpness**	Normal
Compressed Bits Per Pixel	3.324842	**Device Setting Description**	(4 Bytes binary data)
Shutter Speed Value	1/1141	**Subject Distance Range**	Unknown
Aperture Value	2.00	**GPS Version ID**	3.2.0.0
Exposure Compensation	-0.344	**GPS Latitude Ref**	North
Max Aperture Value	2.0	**GPS Latitude**	38.011799 degrees
Subject Distance	0 m	**GPS Longitude Ref**	East

Metering Mode	Center-weighted average	**GPS Longitude**	27.103057 degrees
Light Source	Unknown	**GPS Altitude Ref**	Above Sea Level
Flash	No Flash Function	**GPS Altitude**	19.3 m
Focal Length	3.6 mm	**XP Comment**	0.9.138
Maker Note Unknown	(138 bytes binary data)	**XP Keywords**	N
Flash Pix Version	0010	**Compression**	JPEG (old style)
Color Space	sRGB	**Thumbnail Length**	7,107

Appendix A.2 .Dat File Packet Structure

BYTE	Description	GPS	Motor	Home Point	Remote Control	Tablet Location	Battery	Gimbal	Flight Status	Advanced Battery
0	Start Value	0x55								
1	Message Length	132 bytes	Changeable	46 bytes	55 bytes	Changeable	89 bytes	247 bytes	62 bytes	57 bytes
2	Padding	0x00								
3	Type	0xCF01	0xDAF1	0xC60D	0x9800	0xC12B	0x1E12	0x2C34	0x2A34	0x4411
4										
5	Padding	0x00								
6	Tick Number	4 Bytes integer value of internal clock's packet creation time.								
7										
8										
9										
10	Payloads	Longitude	Unknown	Longitude	Aileron	Unknown	Usable Battery Time	Unknown	Longitude	Unknown
11			Right Front Load							
12					Elevator		Unknown			Rated Capacity
13			Right Front Speed							
14					Throttle					Remaining Capacity
15			Unknown							
16					Rudder					Total Voltage
17										
18		Latitude		Latitude	Unknown				Latitude	Current
19										
20										Capacity Perc.
21										Battery temp(c)
22										Unknown
23										
24										
25										
26		Altitude		Unknown					Altitude	
27										
28									Unknown	Cell Voltage 1
29										
30		Acceleration X	Left Front Load							Cell Voltage 2
31					Mode Switch					
32	Payloads	Acceleration X	Left Front Speed	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Cell Voltage3
33										
34		Acceleration Y	Unknown						FSPitch	Cell Voltage 4

BYTE	Description	GPS	Motor	Home Point	Remote Control	Tablet Location	Battery	Gimbal	Flight Status	Advanced Battery
35										
36									FSRoll	Cell Voltage 5
37										
38		Acceleration Z							FSYaw	Cell Voltage 6
39										
40									Flyc_state	
41					GPS Health					
42										
43		Gyro X							Unknown	
44										
45										
46										
47		Gyro Y								
48					Unknown				Failure	Unknown
49			Left Back Load						No GPS Error	
50										
51		Gyro Z	Left Back Speed							
52									Flight Time	
53										
54										
55		Altitude (Barometer)								
56										
57									Unknown	
58										Unknown
59		Quat W								
60										
61			Unknown	File Ends						
62										
63		Quat X								
64										
65										
66										
67		Quat Y								
68			Right Back Load							
69										
70		Quat Z	Right Back Speed							
71					File Ends				File Ends	File Ends
72	Payloads	Quat Z	0x00	File Ends	File Ends	Unknown	Volt Percent.	Unknown	File Ends	File Ends
73							Unknown			
74		Diff X								

BYTE	Description	GPS	Motor	Home Point	Remote Control	Tablet Location	Battery	Gimbal	Flight Status	Advanced Battery
75										
76										
77										
78		Diff Y								
79										
80										
81										
82		Diff Z								
83										
84										
85										
86		Velocity N								
87										
88								Quat W		
89							File Ends			
90		Velocity E								
91										
92								Quat X		
93										
94		Velocity D								
95										
96								Quat Y		
97										
98		X4								
99										
100								Quat Z		
101										
102		X5								
103										
104								Yaw		
105										
106		X6								
107										
108								Roll		
109										
110		Magnitude X								
111										
112	Payloads	Magnitude Y	0x00	File Ends	File Ends	Unknown	File Ends	Pitch	File Ends	File Ends
113										
114		Magnitude Z								

BYTE	Description	GPS	Motor	Home Point	Remote Control	Tablet Location	Battery	Gimbal	Flight Status	Advanced Battery
115										
116		IMU Temperature								
117										
118		I2								
119										
120		I3								
121										
122		I4								
123										
124		I5								
125										
126		Tracked Satellite No.								
127										
128		Unknown								
129										
130										
131										
132		File Ends						Unknown		
133										
134										
135										
136										
137										
138										
139										
140										
141										
142										
143										
144										
145										
146										
147										
148										
149										
150										
151										
152	Payloads	File Ends	File Ends	File Ends	File Ends	Unknown	File Ends	Unknown	File Ends	File Ends
153										
154										

BYTE	Description	GPS	Motor	Home Point	Remote Control	Tablet Location	Battery	Gimbal	Flight Status	Advanced Battery
155										
156										
157										
158										
159										
160										
161										
162										
163										
164										
165						Tablet Longitude				
166										
167										
168										
169										
170										
171										
172										
173						Tablet Latitude				
174										
175										
176										
177										
178										
179										
180										
181						File Ends				
182										
183										
184										
185										
186										
187										
188										
189										
190										
191										
192	Payloads	File Ends	File Ends	File Ends	File Ends	File Ends	File Ends	Unknown	File Ends	File Ends
193										
194										

BYTE	Description	GPS	Motor	Home Point	Remote Control	Tablet Location	Battery	Gimbal	Flight Status	Advanced Battery
195										
196										
197										
198										
199										
200										
201										
202										
203										
204										
205										
206										
207										
208										
209										
210										
211										
212										
213										
214										
215										
216										
217										
218										
219										
220										
221										
222										
223										
224										
225										
226										
227										
228										
229								rFront		
230										
231								lFront		
232	Payloads	File Ends	File Ends	File Ends	File Ends	File Ends	File Ends	lFront	File Ends	File Ends
233								lBack		
234										

BYTE	Description	GPS	Motor	Home Point	Remote Control	Tablet Location	Battery	Gimbal	Flight Status	Advanced Battery
235								rBack		
236										
237										
238										
239										
240										
241										
242								Unknown		
243										
244										
245										
246										
247										

Appendix A.3 An Example EXIF Data

APPENDIX-3: Curriculum Vitae

Name Surname : Ibrahim GULATAS

Address : Deniz Harp Okulu K.lığı Tuzla / Istanbul

Date of Birth and Place : ANKARA - 04.04.1988

Foreign Languages : English

Education :

Primary School : Kalaba Ilkögretim Okulu, 2002

High School : Naval High School, 2006

Undergraduate School : Turkish Naval Academy, Computer Engineering, 2010

Graduate School : Bahcesehir University, Computer Engineering 2016 - cont.

Career :

Navy Officer (Lt. Jr. Gr.) in Turkish Naval Forces, 2010 - cont.