Drone Forensics: Examination and Analysis

Farkhund Iqbal[1], Benjamin Yankson[2,3], Maryam A. AlYammahi[1], Naeema S. AlMansoori[1], Suaad M. Qayed[1], Babar Shah[1], and Thar Baker[4]

[1]College Of Technological Innovation, Zayed University, Abu Dhabi, UAE
[2]School of Applied Computing, Sheridan College, Oakville, Ontario, Canada
[3]FBIT, University of Ontario Institute of Technology, Oshawa, Ontario, Canada
[4]Department of Computer Science, Liverpool John Moores University, UK

***Abstract*— Unmanned Aerial Vehicles (UAVs), also known as drones, provides unique functionalities, which allows area surveillance, Inspection, surveying, unarmed cargo, armed attack machines, and aerial photography. Although drones have been around for sometimes, mass adoption of this technology is new. The technology is widely adopted in fields including law enforcement, cartography, agriculture, disaster monitoring, and science research. Due to vulnerabilities, and the lack of stringent security implementation, drones are susceptible to GPS spoofing attacks, integrity attacks and de-authentication attacks. These attacks which can allow criminals to access data, intercept the drone and, and use it commit a crime and complicate forensic investigation. The need for standardized drone forensics is imperative in order to help identify vulnerabilities in different models of drones, solve drone related crime, and enhance security; thwarting any anti-forensic measure by criminals. Thus, this paper is presented to report on potential attacks against the Parrot Bebop 2 drone, and the ability for an investigator to collect evidence about the attacks on the drone. This paper aims at examining the possibility of establishing ownership and collecting data to reconstruct events, linking the drone controller with the drone to prove ownership, flight origins and other potentially useful information necessary to identify the proprietor of a crime. In addition, we have also proposed a small-scale drone ontology for modeling drone context data, and simple forensic processing framework for small-scale drones.**

***Index Terms*— digital forensics, investigation, drone security, drone attack, context data, drone ontology**

I. INTRODUCTION

Over the past few years, there has been rapid growth in the interest of Unmanned Aerial Vehicles (UAV) technology. Due to the endless possible uses in civil life, the technology that was once reserved for military use has evolved greatly from a tool for completing dangerous operations such as rescue missions. UAVs, commonly referred to as drones, are aircrafts without any pilots that can be controlled either remotely or autonomously based on a pre-programmed flight path [1]. Currently drones are used in several key applications such as telecommunications relay, police surveillance, border patrol, reconnaissance, inspection of remote power lines and pipelines, traffic and accident surveillance, emergency and disaster monitoring, cartography and mapping, agricultural spraying, aerial photography, promotion and advertising, and fire-fighting [2]. There are also strong interests in the use of drones for commercial transportation.

In 2017, the Roads and Transport Authority of the United Arab Emirates, in collaboration with the Chinese EHANG Company, announced that it had carried out the first test run of a drone, branded as EHANG184, which is capable of carrying a human, in skies of Dubai [19]. Other worldwide companies, such as Amazon, have shown interest in harnessing the benefits of drones, and adopting this new technology as an asset to aid with delivering packages. However, drone benefits do not come without a cost. The pervasive use of drones has spark both technical and societal concern relating to cybersecurity, privacy, and public safety. Drones can be used to collect information that can aid criminals and terrorists in crimes ranging from theft of personal bank details to loss of highly sensitive military recon footage [3]. In addition, they can be used as weapons when programmed to crash into densely populated areas injuring and potentially killing civilians. In 2011, a Massachusetts man was arrested for plotting to fly a remote controlled drone packed with C4 explosives into the Pentagon and the American capital [4]. Also, in 2016, drones forced the airspace around Dubai International Airport to close on three separate occasions - one of which caused delays to 85 flights departing the United Arab Emirates, thus incurring significant costs [20].

As evidenced by these recent events, which are criminal in nature, there is a imminent need for a systematic forensic approach, which would allow us to link a drone to its owner during investigation of such crimes. The need for research in drone forensics is pressing, however research in this area is limited due to a number of challenges. These challenges includes but not limited to: the increased availability of different types of drones; the lack of standardization in drone security; the differences in drone structures, components, and storage media; and finally proper evidence acquisition tools which allows investigator to maintain chain of custody and integrity.

In this paper, we conducted an investigation on a drone controller and the drone itself to determine the possibility of acquiring flight data, extracting media taken by the drone, establishing ownership, and documenting the results of the attack against Parrot Bebop 2 and collecting other evidentiary information. We also proposed a small-scale drone ontology for modelling drone context data, and simple forensic processing framework for small-scale drones. This paper is structured as follows: the Related Work section discusses various papers that have been published in this area of study,

followed by the Experimental Method section that discusses the methodology used to perform the attacks against Parrot Bebop 2. The results of Parrot Bebop 2 investigations are presented in the Result and Discussion section, while a summary of the paper is presented in the Conclusion section

II. RELATED WORK

A. Cyber Attacks Against the Drone

As any other technology, drones are vulnerable to different types of attacks. In a paper Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle Systems", published in 2012, the authors Javaid, Sun, Devabhaktuni, and Alam analyzed various cybersecurity threats against drones systems[5]. The authors deduced that attacks against drone systems are divided into three main categories based on cybersecurity threat models. First, confidentiality attacks deal with unauthorized access to information by compromising the security of communication links between a UAV and its controller [5]. Second, integrity attacks can be conducted through modification of existing information or fabrication of new information [5]. Lastly, availability attack involves jamming, falsifying signals and Denial of Service attacks are some example of cyber-attacks that can be considered a major threat to UAV systems availability [5].

According to E. Vattapparamban, I. Guvenc, A. Yurekli, K. Akkaya and S. Uluagac [6]in their paper "Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety, published in 2016, the common cyber-attacks against drones in 2016 were were De-authentication attacks and GPS spoofing attacks. De-authentication attack can be carried out using an attackers' machine and known IP address of the drone and its controller. The attackers machine sends disassociate packets to the drones controller in order to disconnect it from the drone, which results in losing the connection. This can give the attacker complete control over the drone. This attack compromises the drones' confidentiality, integrity, and availability [6]. GPS spoofing attack on the other hand can be carried out by transmitting fake GPS coordinates to the control system of the drone, which results in hijacking it [6].

B. Drones as Cyber Attack Tool

The previously discussed attacks against drones can be used by malicious entities to conduct physical and cyber-attacks, targeting societies and individuals. According to Kuchler[7], hackers could fly drones outside of corporate buildings and intercept their communications by attacking the corporations Wi-Fi signals, Bluetooth signals and other wireless connections [7]. Such acts could result in collecting sensitive data about the corporation [6]. It is essential to note that many companies who have previously thought of themselves as protected by using their landscapes, or housing data centres in hard to access spaces are now vulnerable to this new threat. In cases such as these, authorities must have the ability to confiscate drones and conduct a forensic analysis in order to identify and locate the owner of the drone used in such a malicious act.

C. Need for Drone Forensics

The aforementioned reasons highlight the imminent need for Drone forensics research to be conducted. This is critical in order to help investigators identify and understand the best methods for collecting and analyzing data related to an attack launched by a drone or launched on a drone. Drone forensics can help investigators reconstruct events and identify potential suspects of a crime. There have been several global incidents where crimes involving drones have gone unresolved due to the fact that investigators have been unable to reconstruct events or trace back to the proprietor of the drone. For example, in 2015 St. Bernardino County in California offered 75,000 dollars in exchange for help in tracking down the owner of a drone who flew over wildfires forcing firefighters to ground aircrafts carrying water to quench the fire[22]. This consequently caused faster spread of wild fire and incurred significant cost to the county. Similar incidents have been reported by Dubai International airport(UAE), Toronto Billy Bishop airport(Canada), and other places across the globe. In all these cases, the proprietors of these drone are still at large due to the inability of forensic investigators to trace back drones involved in a crime.

In 2015 a paper published by Horsman[8] presented results of a digital forensic investigation that was conducted on a Parrot Bebop 1 drone. The investigation was done on the drone itself as well as on the controller. The result shows the ability to acquire data stored in both the drone and its controllers (Galaxy S3 and iPhone 6). In addition, they were able to identify the full movement of both the drone and the controllers during a flight session. Moreover, all storage media content can be extracted along with information such as the longitude and latitude coordinates, and the date of the recording. However, it was not possible to establish ownership of a drone found without its controller (i.e. if a user had abandoned it at the scene of a crime) [8]. This research work focused on only Parrot Bebop 1; however, more research is needed for different types of drones commonly used, as results may vary. This research presents an opportunity for an in-depth look and need for more research into drone and mobile device forensics; since it is common for mobile devices to be used as controls for drones.

In Drone Forensics: Challenges and New Insights H. Bouafif etl., conducted experiment on Parrot AR Drone 2.0[9]. The authors presented the possibilities of acquiring forensic images using four different methods: wireless connections via FTP and Telnet, and direct connections using USB port and serial (UART) port connection. They connected to the Wi-Fi hotspot and performed a port scan using Nmap on the drones IP range. Once scanned, the results showed that connections to a root shell using FTP and Telnet could be established. Exploiting the vulnerability in the drone system architecture, the authors were able to access the operating system files since the root account was not encrypted. Since the USB connection does not allow direct access to the physical disk where the system files and

onboard data reside, a text-based serial console connection using CP210 USB-to-TTL converter was used. In addition, the authors were able to recover flight path data from the mobile controller running the AR.FreeFlight application. Furthermore, they were able to identify the controllers ID in order to establish drone ownership by matching the drones serial number with information found on the controller [9]. Although their work is a great contribution, it did not propose a solution to other core forensics challenges including but not limited to presenting a standard framework for evidence collection, dealing with acquisition and confiscation of drones in an active crime, and gathering information about the attacks and the drone to aid other forensic investigators.

III. EXPERIMENTAL METHOD

The investigation has been performed on the drone controller (i.e. iPhone 6s) and the Parrot Bebop 2 drone to acquire flight data, media recorded by the drone, and ownership information using FTP and iTunes backup. The results show that Parrot Bebop 2 is vulnerable to attacks and that it is possible to link the drone controller with the drone to prove ownership. Lastly, flight origins and other potentially useful information can be found and used to correlate and reconstruct events. For this experiment, Parrot Bebop 2, which was released in November 2015, was used [10]. It includes a dual-core processor with quad-core GPU processor with 8 Gbit RAM and supports Wi-Fi standards IEEE 802.11 a/b/g/n/ac. It can be controlled using various interfaces, such as Android or iOS running freely available software such as FreeFlightPro [11].

The Wi-Fi network of this drone uses a class C IP address in this case 192.168.42.1. It has an open FTP server, which includes images, videos and black box readings [12]. Therefore, it should be possible to perform different kinds of attacks such as de-authentication attack in order to hijack the communication between the drone and paired devices and potentially gaining control of the drone. Furthermore, the open FTP port provides an opportunity to modify media and flight data files resulting in data integrity issues. The test several scenarios looking for possibility of attacking Parrot Bebop 2 and acquiring related evidential information. Here it is possible to establish ownership, reconstruct events, and collect evidentiary information related to an attack against Parrot Bebop 2. Based on current research in the field, we can make the following hypotheses:

- H1: Communication between the drone and paired device can be intercepted in order to gain control of the drone//
- H2: Internal storage of the drone can be accessed to conduct data acquisition
- H3: Data inside the internal storage be manipulated (putting into question its integrity during forensic investigation)
- H4: Ownership of the drone be established with information found on drone's media storage
- H5: Drone events be correlated and reconstructed
- H6: Artifacts from any previous attacks can be acquired

To conduct experiment to prove our set hypothesis based on preliminary findings, we set up a DELL laptop running Kali Linux. This setup was used in order to perform the previously discussed attacks against Parrot Bebop 2. The controller, in this case is a standard iPhone 6s (iOS version) running FreeFlight Pro. Previous backup of controller data was acquired through iTunes backup

IV. RESULTS AND DISCUSSION

A. De-authentication Attack

In order to conduct the attack, the running interfaces of the attackers machine must be active in order to access the interfaces of the drone in order to acquire both the MAC address of the drone and connected controller. Proceeding with this experiment, the Parrot Bebop 2 was turned on and the Linux machine was connected to the drones wireless Bebop-396004. The following setups were executed in order for the attacker to gain controller of the drone:

- The command iwconfig was run to display the wireless network interfaces [13].
- Next, the drones interface wlan was started using the command airmon-ng start wlan0mon.
- Then, the command airodump-ng wlan0mon was run on the same machine to list all the wireless networks in the area, their MAC addresses and other useful information about them.
- Once the drones BSSID was spotted, the process was stopped. With the BSSID Mac address in hand, the next step is run airodump-ng c 6 bssid A0:14:3D:C1:F5:7B w /root/Desktop wlan0mon. In this case A0:14:3D:C1:F5:7B represent the mac address of the BSSID, and the c option in the previous command specifies the channel of the target network. w and /root/Desktop options specify the place where airodump will save any intercepted 4-way handshake, and the wlan0mon indicates the monitor-enabled interface, which enables the capture of more specific information about the Bebop network in order to hijack it.
- Then, when the MAC address of the controlling station appeared, the command aireplay-ng -0 0 a A0:14:3D:C1:F5:7B c 68:DB:CA:BC:EE:8F wlan0mon was run in another terminal simultaneously. This command forces the Kali Linux machine to reconnect by sending de-authentication packets to one of the networks devices(Fig.2), making it think that it has to reconnect with the network. The command is structured as follows: -0 option is a shortcut for the de-auth mode, the 0 means the number of de-auth packets to be sent, -a option indicates the access point/routers BSSID followed by the BSSID of the target network- in this case it was A0:14:3D:C1:F5:7B, -c option indicates the clients BSSID 68:DB:CA:BC:EE:8F (i.e. the device to be de-authenticated), and wlan0mon which indicates the monitor interface as shown in Fig. 1[14].

Following these steps, it was possible to intercept the signal between the Parrot Bebop 2 and its controller iPhone

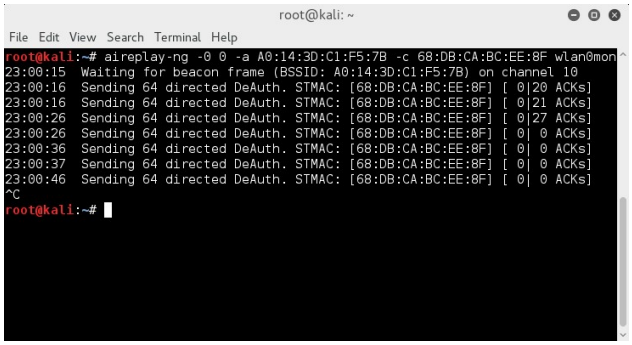

Fig. 1. Sending de-auth packet to intercept the communication

6S. The main controller lost control of the drone and an error message appeared on the display screen of the controller, while the Parrot Bebop 2 fell and crashed. This proves the first hypothesis that Parrott Bebop 2 communication can be intercepted is true. This finding can be used for good and bad endeavor. First, in the case of malicious use, the adversary could have taken control of the drone and used it for other purposes, such as; flying it to commit a crime. On the other hand, during forensic investigation this method can used by law enforcement officers to crash a drone with the intent to to confiscate it for further analysis. Take for instance in Kentucky USA, a man shot a drone with a shotgun because it was flying above his house and he interpreted such as a violation of his privacy. Such rash actions were taken as the man believed that law enforcement was unable to help [22]. Implementing the experimental findings into practice could have allowed law enforcement officers to peacefully resolve such cases. Further, a more interesting novelty and a real world implementation of such will be equipping commercial planes with the ability conduct a de-authentication of a drone that finds itself within a commercial flights flight path, threatening passenger safety. Near misses of an intersection of a commercial planes flight path and that of a drone have been reported to airports across the globe. A clear example of such an incident was illustrated in November 2016, when a major air disaster was narrowly avoided over London skies[20]. A drone nearly collided with an Airbus 320 carrying 165 passengers aboard [20]. Also within the same year, two crew members of a Canadian-based airline, Porter airways, were injured as the aircraft had to suddenly shift in order to evade a drone [21]. In another similar incident, North American Aerospace Defense Command (NORAD) scrambled to deploy a pair of CF-18 fighter jets to intercept a drone which would have interfered with a commercial flight headed to Ottawa, Canada [21]. The implementation of a novel technical intervention such as the aforementioned drone de-authentication technique would quickly, easily, and efficiently allow commercial planes to disengage a drones flight path thus protecting passenger safety. This is critical before the next near miss becomes an true incident.

B. Integrity Attack

To compromise data integrity of the drone, the following steps were carried out:

- The Kali Linux machine was connected to the drones network, then the command iwconfig was used to display the wireless interface connected to the drone network, which in this case was wlan0.
- Next, the command ifconfig wlan0 was used to display the IP address of the drone, which was 192.168.42.86. Once the IP address was determined, the command nmap sn 192.168.42.1 -254 was used to scan the network to list all used IP addresses and the default getaway in the range from 192.168.42.1 to 192.168.42.254. The result shows that the default getaway was 192.168.42.1.
- The command nmap 192.168.42.1 was run to scan the Parrot Bebop 2 for open ports. FTP port was open, a port that can be used to access the internal storage of the drone, which is the port we used to perform the upcoming attack.
- An FTP session was initiated to 192.168.42.1 to gain access to the Parrot Bebop 2s internal storage. It appears that once the connection was initiated, root shell privilege was gained. Files and directories in the internal storage were accessible, which confirms the second hypothesis because videos and photos taken by the drone. Figure 2. demonstrate successful download of content of internal storage media.

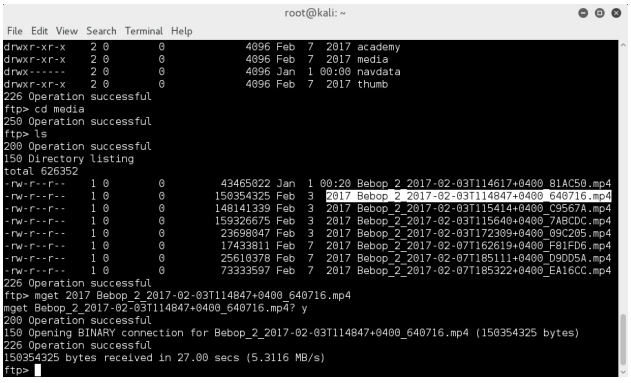

Fig. 2. Downloading video to the attackers controller

- Additionally, the command mput was used to upload the file hacked.jpg to the drones internal storage as shown in Figure 3.
- The root privileges gained by the initiated FTP session enables the deletion of files from the Parrott Bebop 2 using the command delete as shown in Figure 4
- Moreover, the root privilege enables renaming the files of the the Parrott Bebop 2 as shown in Figure 5, which confirms the third hypothesis that the files in the Parrot Bebop 2 can be easily accessed and manipulated.

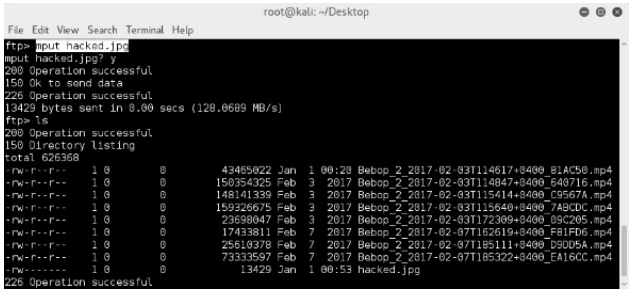

Fig. 3. Uploading photo to the drone

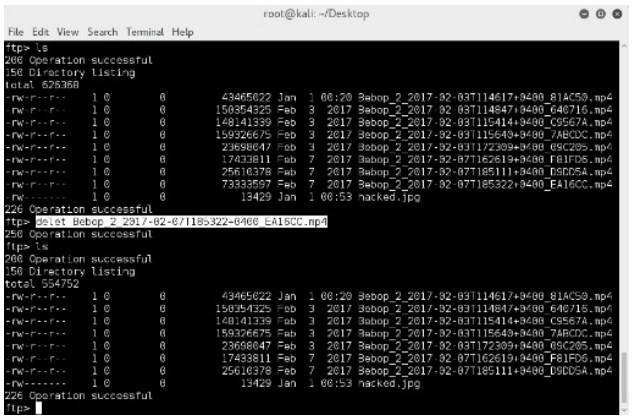

Fig. 4. Deleting a file from the drone through FTP

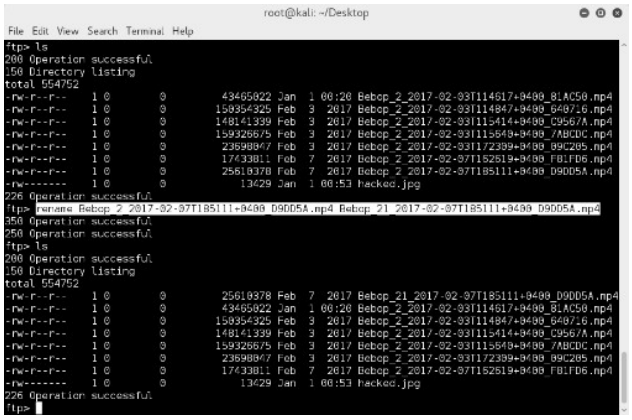

Fig. 5. Renaming a file of the drone through FTP

C. Data Acquisition

There are several methods of data acquisition for iPhone forensics. Such methods include using commercial tools such as oxygen, XRY, and using the dd command in Linux as illustrated by Zdziarski [15]. Figure 6 presents an ideal acquisition and process structure that begins with confiscation through data acquisition and follows through to the forensic analysis that should be followed for small-scale device forensics.

Figure 6 proposes an ideal framework for forensic analysis of small-scale drone. It begins by determining the status of the drone; this can vary between running state, crashed state,

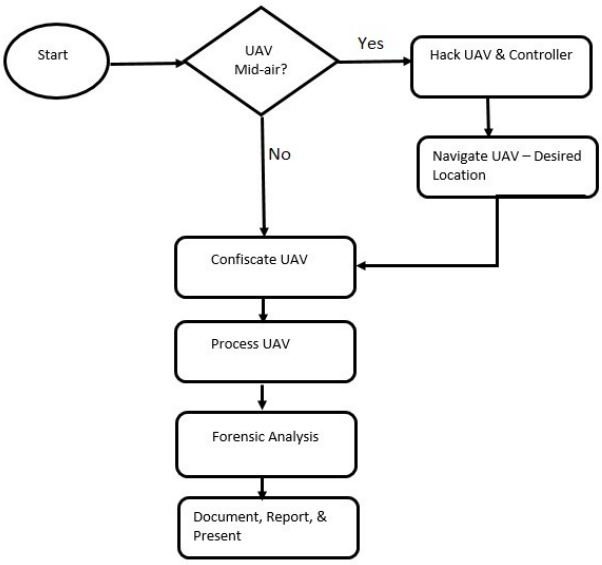

Fig. 6. Proposed simple forensic processing framework for small-scale drones

or operational state. If the drone is crashed within a crime scene, then law enforcement can proceed by confiscating the device. If the device is mid-air then law enforcement can use this proposed approach to de-authenticate the drone, take control of it, and confiscate it. Under both circumstances, the proper legal forensic best practices of seizure should be followed. This is to say that law enforcers have the correct authorization or required warrants to conduct the confiscation. Once confiscated, law enforcement can proceed with analysis of the drone. In processing the device, basic steps such as preparation, identification, collection, and customization must be adhered to. This is done by accessing the risk to investigation, identifying obvious physical evidence on the drone (which may lead to the owner), identifying system capability of the drone and identifying technical requirements and tools needed to conduct forensics analysis. During the forensic analysis phase, with the set of forensic tools identified for investigation, it is necessary to analyze the WIFI connection information between drone and controller, the geo-location data from the drone, the storage, the camera and all other areas within the drone where data is processed. The documentation must be completed, a report compiled, and findings presented during the final phase. In our research, we followed our proposed simple approach for forensic processing framework for small-scale drones. Firstly, the data was acquired from the iPhone 6S used to control the drone via iTunes backup [16]. The backup is stored in the AppData file located on the C: drive as shown in Figure 7.

The .plist files, i.e. property list files, contain various kinds of information such as basic device information, applications used on the iPhone and configurations [17]. In order to ensure the integrity of the evidence, the SHA-1 value was calculated and compared with the latter-calculated hash value after the analysis was completed as shown in Figure 8 below

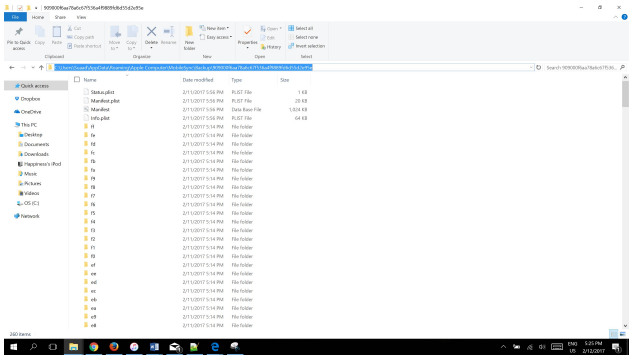

Fig. 7. iPhone backup via iTunes

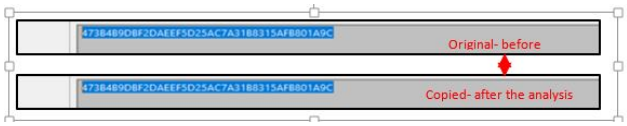

Fig. 8. 1 hash value

In order to recover the images and videos from the drone, a Kali Linux machine was connected to the drone through FTP. The main file containing the data is called internal _000. It contains 6 main directories, some of which contain files and subdirectories. The following diagram(Figure 9) shows the hierarchy of the directory internal _000.

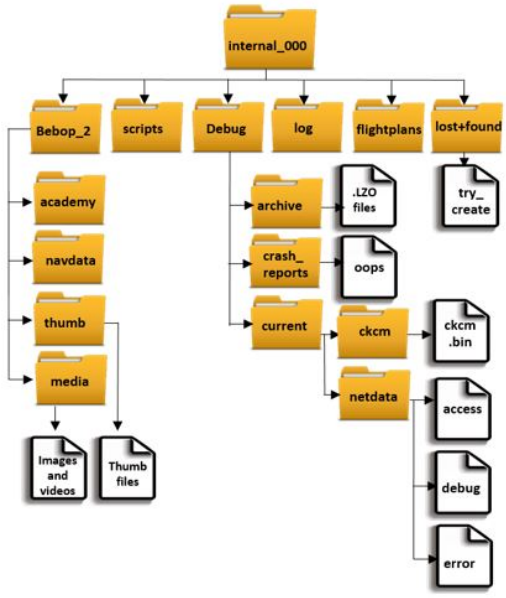

Fig. 9. Hierarchy of internal file

This depicts a clear delineation that no security measure is in place to provide secure authentication or to protect stored data integrity. This is a good indication that an adversary can easily manipulate data for malicious purposes or used this technique as an anti-forensic measure - further complicating the forensic investigators work.

D. Forensic Analysis

In analyzing the Controller, in this case the iPhone 6S, since the majority of the data in the backup is encrypted, the attempt of using SQLite viewer software was not successful. Therefore, the files were examined individually to identify the information that can be potentially critical to an investigation. The basic information about the iPhone 6S device such as the device name, GUID, IMEI, installed applications and serial number was found in the info.plist file. By analyzing the files, traces of the identity of the drone owner were found. The Apple ID used to download the application that was used to control the drone was found. In addition, more information about the Apple ID and region was found as shown in Figure 10.

```
maryam.it@hotmail.com_DLEDC1urn:ds:1142244903_
AE^+9710000000000BS\D:1142244903_DLE$41201F62-
```

Fig. 10. Apple ID and region extracted from the log files

Furthermore, the first name and last name associated with the Apple ID was identified as shown in Figure 11. This helps in identifying the drone operator's identity

```
FirstName_DLEFSAccountAvailableService
AccountSourceZDSPersonIDXLastName_DLE.
Maryam_DLENAKmaryam.it@hotmail.com
BSVdeviceDC2DNAKF'WYammahiNULBSNUL
```

Fig. 11. First and last name associated with the Apple ID

In addition to associating the region with the Apple ID account and identity of the account owner, correlating the drone with the iPhone was possible. There were several files in the backup data that list the flight dates and times with the serial numbers of the drones that used for the flights. Figure 12 shows an example of a flight on 07/02/2017, where the time was 4:26:19 PM, GMT +4 (i.e. the UAE time zone). This confirms the fourth hypothesis; the ownership of the drone can be established with information found on drones media storage.

```
2017-02-10T113227+0400_DLEDC2PI040376AA6A396004_DLE
DLESYN2017-02-07T185322+0400_DLEDC2PI040376AA6A396004
2017-02-07T185111+0400_DLEDC2PI040376AA6A396004_DLE
2017-02-07T162619+0400_DLEDC2PI040376AA6A396004_DLE
```

Fig. 12. Linking the drone to the flights

Since commercial tools for extracting data from the iPhone was not used, finding the deleted videos and images was not possible via iTunes backup. However, the record of the number of flights and the total flight time was found as shown in Figure 13. This can help investigators in determining the number of videos expected to be found in the drone and queue them to look for logs to find GPS coordinates and other information of deleted flights which may also be relevant to an investigation

Through further analysis, it was also possible to find the GPS coordinates of the flights taken. Figure 14 shows basic

```
Flight infos:
Last error: 'No error detected'
Number of flights:        86
Previous flight time: 0 days, 0 hours, 0 min, 31 s
Total flight time:    0 days, 0 hours, 26 min, 47 s
```

Fig. 13. Information about drone flights

information about the flight and the drone such as: the serial number, UUID, and drone controller, date and time of the flight, and location information. Such information can be crucial to forensic investigators in order to correlate a suspect using the drone with a specific time and location.

```
"date": "2017-02-07T162619+0400", "product_id": 2316,
"serial_number": "PI040376AA6A396004",
"product_name": "Bebop 2",
"uuid": "F81FD6D0253DE7FCEBFD69D3ABA4F700",
"run_origin": 0, "controller_model": "iPhone",
"controller_application": "com.parrot.freeflight3",
"product_style": -2, "product_accessory": -2,
"gps_available": false, "gps_latitude": 24.409412,
"gps_longitude": 54.608611, "crash": 0, "jump": null,
```

Fig. 14. Basic information about the flight

During the experiment, the drone was flown from four different locations: three within Abu Dhabi City and one within Alain City. Upon further analysis, all four locations from where the drone took off were identified. Figure 15 shows the takeoff location in Al Ain, while Figure 15 shows one of the locations in Abu Dhabi. The files that contained this information also contained the date of the flight, which makes correlating such information even easier. The above scenarios can be used to prove the fifth hypothesis; the ability to correlate and reconstruct events.

```
TAKEOFFSUBÔÛSTXMAND(ETBa    òÈVTCANBS´c'äETX
2eFFGÐSO88SO+>ETX%[%DñSOH] DeRSON~co#hÓSOHates',²Î%(FS>DLE +lSOHBEL/
GPS PILOT"µ&iŒ|SUB@±ENQto: 24.2SUBh     8, 55.700025ÕFF5
```

Fig. 15. Take off location in Al Ain City

```
 event: TAKEOFF_%FØ(3SYNENQ'
jSOH%[NAKHsBS] Device coDC3lXSOHatesETBDLE/ÙSYNA
lSOHFF/GPS PILOT posiŒ|ãNULACKto: 24.409472, 54.608595ÕF
```

Fig. 16. One of the take off locations in Abu Dhabi City

From the acquired backup files, the image inserted in the attack and the renamed file were found in the internal _000 file. This shows how easy it can be for attackers to manipulate potential evidence as shown in Figure 17.

Bebop_21_2017-02-07T185111+0400_...	2/12/2017 11:11 A...	MP4 File	25,011 KB
hacked	2/12/2017 11:09 A...	JPG File	14 KB

Fig. 17. Renamed and inserted files

Since the drone was hacked using a de-authentication attack, traces of the attack were found in the log files. Disassociation packets were sent to the controller (MAC address 68:db:ca:bc:ee:8f) as shown in Figure 18 below; this proves the sixth hypothesis that artifacts from previous attacks can be acquired.

```
DETECTED :GS„Z  DISASSOC_INDDC4 HNULEOT68:db:ca:bc:ee:8f
```

Fig. 18. De-authentication attack

E. Drone Context Data Model

There are various ways we can model context data for drones to understand drone data. The drone context data model will help forensic investigators clearly understand the types of data available and how best to proceed with the investigation. To understand drone context data, we need to adopt existing data models, and propose a data models which will best fit drone data. The context data models in consideration for drone data:

- The Key Value Model This is a simple data model where information is represented using tuples. In this case key value pairs can be used to describe the capability of a services provided by the drones. Service discovery of the drone can be applied by using matching algorithms.
- The Markup Scheme Model - This model can also be considered for drones, but is not ideal because the model comprises of having a hierarchical data structure made up of mark-up tags, which includes attributes and contents. The contents of the tags are usually recursively defined by other tags [23].
- The Logic Based Model - This model can be considered as theoretically desirable approach to model context data for drones, but complexity in its implementation can be an impediment. Facts expressions and rules are generally used to define a context data model. Logic based system are then used to modified (update, delete, add) new fact. To gather ongoing new facts about the context, reasoning is used to deduct new facts based on existing rules [23].
- The Object Oriented Model - This model is a more appropriate model to analyze context data model for a drones as compared against Key Value, Mark up Scheme or Logic Based. In this situation, objects are used to represent different context types that encapsulate processing and representation. Context data is accessed using well-defined set of interfaces.
- The Ontology Based Model - This data model will be the best to model drone context data. Although most of the discuss data modeling approach can be used, Ontology Based Model is the best for modeling drone context data when evaluated against key criteria such as simplicity, flexibility, genericity and expressiveness. This is because an ontology based model represents a description of concepts and relationships. It is a formal specification between terms and relations. Data is extracted through applying ontology-reasoning techniques. As discussed by Bimal Aklesh Kumar [23] the following will be appropriate description of comparative data model as illustrated in Table 1. To illustrate that Ontology Based Model will be the ideal model to use for drone data, we can analyze drone data based on

the information provided the comparative data models. As per Table 1, the following key criteria should be considered: Simplicity, which stipulates that expressions used should be simple and easily understood. Flexibility adjudicates that data model should easily support the inclusion of new context entity and relationship. Genericity accepts that the data model should not be limited in supporting only certain context information rather various types of context information should be supported. Finally, Expressiveness looks at allowing as much as it can be allowed, a detail description of context [23].

REQUIREMENTS	CONTEXT DATA MODELS				
	KEY	*MARKUP*	*LOGIC BASED*	*OBJECT*	*ONTOLOGY*
SIMPLICITY	YES	YES	NO	NO	YES
FLEXIBILITY	NO	YES	YES	YES	YES
GENERICITY	YES	YES(Limited)	NO	YES	YES
EXPRESSIVENESS	NO (Complex algorithms)	NO (Performance problems)	NO(Data quality issues)	NO(Query issues)	YES

Table 1 – Comparison of existing data models.

Table 1 provides us a building block in analyzing and selecting the best context data model for drones. The Key Value Model will successfully pass for Simplicity, Generality but will have challenges dealing Flexibility from recreating new models from existing data. It also lacks ability to express capability to support complex algorithms, which is essential drone context data as we expect contest information will consistently change as a drone flies around. Therefore, ideally it will be cautious in case not to model drone context data after it.

The Markup Scheme Model easily passes Simplicity as it uses XML implementation. It passes Flexibility as it supports Resource Description Framework (RDF). RDF comes in handy for drones context data modeling. Unfortunately, the model does not fully pass Genericity or Expressiveness. The Markup Scheme Model has limitation on the type of context data it can support and when query large set of data can be problematic on performance. An impact on performance can be disastrous in drones where the ability to maintain consistence performance is essential to the operation of the drone itself.

The Logic Based Model fails for simplicity. It is quite challenging to implement as it is based. It fails for Flexibility also as it is hard to build new logic from existing one. Finally has high level of formality but suffers from lack of Expressiveness and supporting the quality of contextual information [23]. Any unavailable or missing contextual data will be is difficult to address. Further deduction shows that this model is error prone in it its applicability to an existing mobile computing environment. It is very challenging because full logic reasoners are usually not available [23]. but the Object Oriented Model passes for Flexibility, Genericity and Expressiveness but fails in Simplicity due to the complexity of managing context data as object. This model provides encapsulation to the details of context processing and representation. At times, it becomes a tedious task to query and obtain the desired result [23].

The Ontological approach to context data easily passes all the criteria. For simplicity, it is very simple to create and maintain context data using ontologies. It also allow reused of data which will be essential to drone context model as it provide the high degree of Flexibility. Further new ontologies can be easily created among existing ontology there by satisfying Genericity by supporting various types of context information. Finally yet importantly, it easily supports reasoning providing a good impetus support as much as possible a detail description of context information by the drone. The key rationale to model drone that with Ontologies is that Ontologies offer flexibility and extensibility and are naturally suited to distributed systems, as they may be stored at different places and created by different authors. In context modeling, ontologies can be used to describe drones environment, activity, owners information, and services.

Overall using ontology methodology to model drone context data, allows us to easily see which context information is easily susceptible to an attack and how such information can be encapsulated to protect and prevent such an attack. In addition, authorities can use this information during a forensic investigation to trace the drone back to the owner in a case where the drone has been found to be involved in an illegal activities. There are particular drone context information, such as drone owners information, that may not be available in all geographical areas, but since our experiment was conducted in the United Arab Emirates where it is required by law to register all drones, such information is available.

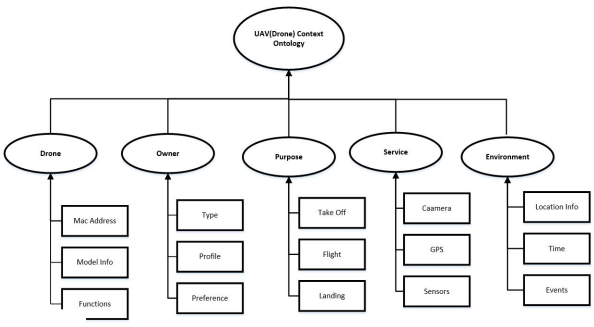

Fig. 19. Ontology based context data model for drones

We have develop Figure 19 to depict an ontology of a drone as a model for context data, which presents the following information:

- Drone Information basic identifiers about drone (Mac Address, model, type, year, services)

- Drone Owner Information information about users profile (User Type, Name, Age, date of purchase, Address, license number, Preferences)
- Services describes the types of services drone provide required by the user (Hobby drone, Imaging, Data Collection, surveillance, etc.).
- Activity describes the type of information required by the drone (Flight Take off information, In flight information, landing information).
- Environment describes the environment related properties (time, location etc.)

V. Conclusion

With the recent overwhelming increase use of drones, the need for drone forensic analysis has become a necessity. Sparse research has been conducted in the field of drone forensic analysis and much more work is required in order to create tools that will aid with law enforcement and for use in cases of public safety. This paper briefly discusses different research papers that have been published in the area of drone forensic analysis. An experiment of two different types of popular attacks against the Parrot Bebop 2 has been conducted in order to determine the ability to collect evidentiary information about these attacks. Firstly, the de-authentication attack has been conducted by hijacking the communication between the drone and its controller using Linux command and IP address of the drone and its controller. This type of attack could be a useful tool to help law enforcers in dealing with drone acquisition and confiscation in situations where drones are involved in a crime and before further forensic analysis can be conducted. Secondly, the integrity attack has been conducted through establishing a wireless connection via FTP in order to modify the existing information and fabricate new information. This type of attack could be used maliciously and could easily complicate or mislead a forensic investigator.

Acquisition of evidential information related to the attack against the Parrot Bebop 2 has been done using FTP and iTunes backup. Therefore, the analysis of the acquired data showed that the Parrot Bebop 2 is vulnerable to attacks. Moreover, it was proven that it is possible to link the drone controller with the drone to prove ownership, and determine the flight origin and other flight information to correlate and reconstruct events. The proposed a small-scale drone ontology for modeling drone context data, and simple forensic processing framework will allow investigator to understand drone context data and follow a simple framework during investigation. In the future, the development of forensic tools using this knowledge could easily be used to acquire and analyze data from both the drone and its controller in conjunction with other investigative techniques.

References

[1] T. Matiteyahu, "Drone Regulations and Fourth Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy," Columbia Journal of Law and Social Problems, pp. 48-265, 2015.

[2] A. Cavoukian, Privacy and drones: Unmanned aerial vehicles, Ontario: Information & Privacy Commissioner, 2012.

[3] N. D. C. &. C. K. McKelvey, "Drones and Privacy," International Journal of Handheld Computing Research (IJHCR), vol. 6, no. 1, pp. 44-57, 2015.

[4] . Johnson, "Man accused of plotting drone attacks on Pentagon, Capitol," 29 September 2011. [Online]. Available: http://usatoday30.usatoday.com/news/washington/story/2011-09-28/DC-terrorist-plot-drone/50593792/1. [Accessed 20 January 2017].

[5] A. Javaid, W. Sun, V. Devabhaktuni and M. Alam, "Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System," in IEEE Conference on Technologies for Homeland Security (HST), Greater Boston, 2012

[6] E. Vattapparamban, I. Guvenc, A. Yurekli, K. Akkaya and S. Uluagac, "Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety," in International Wireless Communications and Mobile Computing Conference (IWCMC), Cyprus, 2016.

[7] H. Kuchler , "Cyber experts warn of hacking capability of drones," 31 July 2016. [Online]. Available: https://www.ft.com/content/a06a1f5c-505f-11e6-8172-e39ecd3b86fc. [Accessed 2017 February 2].

[8] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," Digital Investigation, no. 16, pp. 1-16, 2015.

[9] H. Bouafif, F. Kamoun, F. Iqbal and A. Marrington, "Drone Forensics: Challenges and New Insights," ADFA, 2011.

[10] "Bebop 2 vs Bebop Drone comparison," 12 January 2016. [Online]. Available: http://blog.parrot.com/2016/01/12/comparison-bebop-2-vs-bebop-drone/. [Accessed 10 February 2017].

[11] "Parrot BEBOP 2," [Online]. Available: https://www.parrot.com/ca/drones/parrot-bebop-2#technicals. [Accessed 9 February 2017].

[12] "Parrot Bebop Drone Hacking," 9 December 2014. [Online]. Available: https://github.com/AutonomyLab/bebop_hacking/blob/master/README.md. [Accessed 9 February 2017].

[13] "iwconfig.," [Online]. Available: http://www.linuxcommand.org/man_pages/iwconfig.8.html. [Accessed 9 February 2017].

[14] L. Encarnacion, "How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng," [Online]. Available: http://lewiscomputerhowto.blogspot.ae/2014/06/how-to-hack-wpawpa2-wi-fi-with-kali.html. [Accessed 9 February 2017].

[15] J. Zdziarski, "IPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets," "O'Reilly Media, Inc.", Sebastopol, 2008.

[16] T. Proffitt, "This is a GIAC Gold Template Forensic Analysis on iOS Devices," SANS, 2012

[17] B. Satish, "Forensic analysis of iPhone backups," [Online]. Available: https://www.exploit-db.com/docs/19767.pdf. [Accessed 10 February 2017]

[18] "Emirates calls for tougher action on drones after airport closures — The National", Thenational.ae, 2017. [Online]. Available: http://www.thenational.ae/uae/emirates-calls-for-tougher-action-on-drones-after-airport-closures. [Accessed: 24- Apr- 2017].

[19] C. Milmo, "Drones used to deliver illicit goods to prisons, say senior officials", The Independent, 2017. [Online]. Available: http://www.independent.co.uk/news/uk/crime/drones-operated-by-criminal-gangs-used-to-deliver-drugs-mobile-phones-and-potentially-firearms-to-10504154.html. [Accessed: 23- Apr- 2017].

[20] Air disaster narrowly averted over London after drone nearly collides with plane", The Sun, 2017. [Online]. Available: https://www.thesun.co.uk/news/2200187/major-air-disaster-narrowly-averted-over-london-after-drone-nearly-collides-with-passenger-plane-near-the-shard/. [Accessed: 24- Apr- 2017].

[21] L. News and O. Andrew Seymour, "Near-collision with possible drone injures crew members on Porter flight from Ottawa", Ottawa Citizen, 2017. [Online]. Available: http://ottawacitizen.com/news/local-news/flight-crew-injured-after-near-collision-with-suspected-drone. [Accessed: 23- Apr- 2017].

[22] Judge rules man had right to shoot down drone over his house", CNET, 2017. [Online]. Available: https://www.cnet.com/news/judge-rules-man-had-right-to-shoot-down-drone-over-his-house/. [Accessed: 22- Apr- 2017].

[23] B. A. Kumar, Ontology based data model for context aware mHealth application, Next Gener. Comput. Technol. (NGCT), 2015 1st Int. Conf., no. September, pp. 274279, 2015.