Forensic Analysis of Popular UAV systems

Thomas Edward Allen Barton and M A Hannan Bin Azhar
Computing, Digital Forensics and Cybersecurity
Canterbury Christ Church University
Canterbury, United Kingdom
Email: tb1150@canterbury.ac.uk; hannan.azhar@canterbury.ac.uk

Abstract— **Recent and sudden rise in the popularity of drones or UAVs (Unmanned Air Vehicles) can be attributed to the reduction in weight of electronic components and the relative ease by which the drones can be operated. Their potential applications range from simple leisure and recreational purposes to photography, transport, surveying, security, the list goes on. With this demand and subsequent availability, there has also been a rise in drones used in crimes. This creates a need for forensic analysis into these devices, which often use custom electronic flight systems for which appropriate forensic tools have not been developed. This paper covers the use and development of open source tools to aid forensic analyses of two popular drones - the DJI Phantom 3 Professional and AR Drone 2 with the aim of reconstructing the actions taken by these drones, identification of owners or operators, and extraction of data from associated mobile devices. While different UAV systems can vary in their operations owing to their capabilities, some generic methods will be used in analyses and extractions of the data and then results will be compared between models.**

Keywords—digital forensics; drone forensics; Linux, DJI Phantom; AR Drone 2.0; open source tools.

I. INTRODUCTION

Reports of drone-related incidents in the UK rose by 352% between 2014 and 2015 [1]. The growing availability and popularity of such devices means drone crime is an inevitability, and is likely only going to increase in the future. The wide potential applications of a drone means there is no one type of crime being committed, however the current climate is dominated by the transport of contraband. Smuggling offences committed both in domestic and international territories have demonstrated that drones are a capable and efficient delivery method, whatever the cargo. In the UK, drones are being used to smuggle weapons, phones and drugs into prisons, items which all have highly inflated value [2]. Worldwide, drones are being used to bypass borders, such as the United States/Mexico border where drones have been recovered carrying cargos of marijuana, heroin and methamphetamine as well as small weapons [3].

As well as smuggling, camera equipment that is commonly mounted to UAVs raises a host of privacy concerns. In most cases cameras are implemented either as static recording devices, or for live streaming (sometimes known as vision). Many different areas of airspace in the UK are designated no-fly zones [4] because they are considered "sensitive areas" – these include sites such as airports, military bases and power stations. The ability of drones to capture pictures and videos of operations in these sites presents a significant security threat. As well as the security of infrastructure, individual security may also be compromised. Of the reported incidents mentioned earlier, 257 were simply concerns for public safety [1]. As well as simple privacy violations, drone-mounted cameras can also be used as an aid to traditional crime, such as burglary [5].

A modern drone is capable of carrying loads of up to 8kg [6] over vast distances, and is often equipped with an array of on-board sensors and other electronics that assist with flight and navigation, as well as camera equipment and digital storage. This makes drones a valuable source of forensic artefacts, creating the need for forensic research into the area. This paper will cover the forensic analysis of two popular drones; the DJI Phantom 3 Professional (Phantom) and the A.R. Drone 2.0 Power edition (A.R). Among commercially available drones, DJI has taken the largest market share of 36% [7] with its Phantom series setting the benchmark for professional drone use. A.R has a large range of drones available with many different features. While these drones are different in their operation owing to their capabilities, some generic methods of analysis can be applied to many different models. The methodology used in this paper will focus on these generic methods and compare the results between models.

The remainder of the paper will be organised as follows: Section 2 will discuss existing research in relation to drone forensics, covering the drones featured in this paper. The methodology used during the analysis process will be discussed in Section 3, including acquisition and analysis of mobile, flight data and media artefacts for both platforms. Section 4 will cover the results of the analysis. Finally, Section 5 will conclude the paper and mention possible future work.

II. RELATED WORK

Some important aspects of drone forensic analysis have been highlighted, including establishing flight data and establishing ownership [8]. These present a variety of challenges to the digital forensic investigator. Firstly, the interpretation of flight data is an essential part of drone forensics, and requires a skillset that is not normally possessed by a forensic analyst. Secondly, the presence of identifying artefacts such as names and addresses is not essential for the operation of the drone. This is a stark comparison to mobile forensics, where devices provide an abundance of personal information. In a crime scenario, there will be no inclination to provide such information and it is unlikely to be present. Artefacts have

been successfully recovered from the DJI Phantom 2 Vision+, including flight data and recorded media - using mobile forensics to acquire data from the DJI GO controlling application, and using cyber security techniques to gain access to the internal storage of the UAV [9].

Drones, like smartphones, are fully integrated digital systems with their own storage, processing and network capabilities and must be treated as such. Analysis of storage media is where traditional digital forensic techniques become useful. The recorded media of the Phantom 2 Vision+ was found to possess Exchangeable Image Format (EXIF) metadata including GPS (Global Positioning System) information [9]. In the absence of flight logs, co-ordinates extracted from EXIF data can be used to recreate a flight. Cyber security techniques are often used to gain access to data and components where chip-off analysis is not available. Analysis of the Phantom 3 Standard edition revealed that an IPv4 network is created between the components of the UAV system including the drone, controller, on-board camera and smartphone. De-compilation of the DJI GO application revealed the Service Set Identifier (SSID) and password required to gain access to this network [10].

A.R drones use an embedded Linux operating system that governs the flight, camera and network interfaces. The drone provides an unsecured (by default) wireless access point. Once connected, root access to the operating system is granted via an anonymous telnet port. Root access presents a number of options for acquisition, including imaging internal storage partitions and logical-level copying [8]. While methods to analyse specific models of drones have been successful, this paper will focus on some generic methods that can be applied to both the DJI Phantom 3 Professional and the A.R. Drone 2.0 Power edition.

III. Methodology

This paper focusses on two drones and one mobile platform, as shown in Table 1 and Table 2 respectively. The Phantom 3 Professional is a high capability commercial drone capable of traveling long distances and while the A.R Drone is more affordable, it still is capable of hovering and capturing imagery which gives it the potential of committing crime.

TABLE I. Drones

Name	**Specifications**			
	Price	***Weight***	***Camera Resolution***	***Range***
DJI Phantom 3 Professional	£699.99	1280g	4K (12 Megapixels)	5Km
A.R Drone 2.0	£299.99	380g / 420g	720p (0.9 Megapixels)	50m

TABLE II. Android Mobile Platform

Name	**Specifications**			
	Model Number	***Android Version***	***CyanogenMod Version***	***Installed Applications***
Motarola Moto G 3rd Generation	MotoG3	5.1.1	12.1	DJI GO v3.1.4 , A.R Freeflight v 2.4.15

To generate the required data for acquisition and analysis, a scenario was created on the devices by simulating the use of the drones in a crime. A suitable remote area with some high story buildings and open space was chosen to test the capabilities of the drones. Four waypoints over about a 150m radius were established. Once data was collected, the drones and the mobile platform were analysed in a digital forensics lab. Because of the multi-platform nature of UAV systems, no one forensics toolkit was suitable for analysing acquired data. For this reason, open source and custom tools were used throughout the acquisition and analysis process. These provide some significant advantages over commercial toolkits such as the ability to be tested by the open source community, meeting what are known as the "daubert" guidelines for the admissibility of evidence provided by expert witnesses [11]. Furthermore, custom tools created by the forensic investigator to perform a specific job are highly adaptable and, where successful, can be used again in other cases involving similar technology. A forensic workstation running Kali, a distribution of Linux with several forensics and cybersecurity tools was used as well as a workstation running Windows, as listed in Table 3.

TABLE III. Forensic Workstations

Name	**Specifications**
	Operating System
Toshiba Sattelite L450D	Kali Linux Rolling Update
Fujitsu LB A512 NG Core I3	Windows 10

The analysis later performed was divided into three categories; Mobile forensics, flight data and media. As modern drones are controlled through an application running on a mobile platform, the forensic analysis of these applications is paramount when analysing drone systems. Flight data is used to recreate the actions of a drone during flight, which is especially important when the drone has been used in smuggling or other flight-related crime. Finally, the media captured by the drone has forensic value in not only tracing the drone to its location during flight but also in cases of invasion of privacy.

A. Mobile Forensics

Mobile forensics covered in this paper relate to artefacts recovered from the DJI GO and A.R Freeflight applications installed on the mobile platform using mobile forensics techniques. An open-source operating system, CyanogenMod [12] provide rooting, which is necessary to access portions of internal storage that are protected by the operating system's security [13]. The chosen operating system was used because the root access was granted natively, rather than needing to install third-party rooting software, which is a forensically sound option when methods such as chip-off analysis are not available. Although CyanogenMod differs in the features it provides to users compared to stock operating systems, the methods used to acquire data from the mobile platform are generic and can be applied to all Android systems [13]. Once

the test platform was connected to the forensic workstation, root terminal access was granted using Android Debug Bridge (ADB) [14]. The "userdata" partition was identified by running the command "ls /dev/block/bootdevice/by-name" as being "mmcblk0p42", as shown in Figure 1. A forensic image of this partition was then created using the "dd" Linux utility, and stored on a removable storage card formatted in the "ExFAT" (Extended FAT) filesystem. This was then copied to the forensic workstation for analysis.

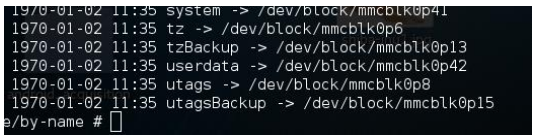

Fig. 1. Listing of mounted partitions on Android Platform

B. Flight Data

Flight data was collected via various sensors present on the UAV systems. Some key data of interest were GPS readings, altitude, speed, acceleration and battery levels. Analyses of these data can reveal the actions taken by the drone and can be used to re-construct flights. Flight data was stored on either the UAV internal storage or the mobile application, sometimes with copies on both. Recovery of data from the UAV internal storage required interfacing with access routes provided by the UAV platforms.

1) DJI Phantom 3 Professional

The DJI Phantom's internal storage exists in the form of a micro SD card semi-permanently mounted to the main board of the UAV [14]. While chip-off forensics through removing this card would be the most forensically sound option of data acquisition, this was not chosen as it would impair the functionality of the drone. Instead, the UAV was placed in "flight data" mode through the DJI GO application, which makes the card accessible through the UAV's micro USB port. The UAV was connected to the forensic workstation and an image of the internal storage was created. As the DJI Phantom's system stores flight data in a proprietary format [15], it is necessary to use a tool for analysis. Many online services offer interpretation of DJI flight data, but uploading files to an externally hosted server is not appropriate for forensic investigation purposes. For this reason, an open source tool, "CsvView" [16] was installed on a forensic workstation running Windows and connected to the internet. Established with a google API key, the tool is able to download imagery from the Google Maps service.

2) A.R Drone 2.0

Unlike the DJI Phantom, the A.R drone does not have any hardware ports that allow access to the internal storage, which presents as a flash chip permanently mounted to the main board of the UAV. With chip-off analysis being unavailable in this case, the UAV was connected to the forensic workstation through Wi-Fi, which is a method used by both digital forensics and cyber security researchers to acquire data and investigate the drone [8]. When switched on, the UAV becomes a Wi-Fi hotspot with no form of authentication. Acquisition using this method will invariably change data on the device, so all actions were performed in accordance with the Association of Chief Police Officers (ACPO) guidelines for handling digital evidence, specifically principles 2 and 3. Once connected, the forensic workstation's Address Resolution Protocol (ARP) was queried, revealing the UAV has a local address of "192.168.1.1". Running "nmap" [17] against the UAV revealed a telnet port, and root access was gained. Because of complications relating to the UAV's Unsorted Block Image file system (UBIFS), logical level copying over the network was favoured over physical imaging.

C. Media

In the case of both the DJI Phantom 3 and the A.R Drone, media, including photos and videos taken by the UAV's on-board cameras, was stored on a removable storage. In the case of the DJI Phantom, this was a micro SD card slot on the main body of the UAV, which came pre-installed with a 16GB card. For the A.R Drone, a standard USB port was present next to the battery inside the hull of the UAV, which a flash drive was connected to. Both of these removable storage media were connected to the forensic workstation and images were created. While the media itself was examined using standard image viewing software present on the forensic workstation for consistency, a third party open-source tool, "exiftool" [18], was used to analyse the metadata of media files. This command-line tool presented the data in a raw, detailed format and the formatted output was easily manipulated using scripts.

IV. Results

The results cover the key findings from the analysis described in the previous section. The results are presented with regards to the three categories of artefacts; mobile data, flight data and media.

A. Mobile Forensics

The mobile applications for each drone platform contained a wealth of artefacts. These not only include identifying artefacts such as account names or e-mail addresses but also flight data and media, making correlation between the UAV and mobile application possible through comparing artefacts.

1) DJI Phantom 3 Professional

A number of useful directories were located within the "media/0/DJI" directory on the "userdata" partition. A list of these with descriptions is shown in Table 4. The serial number for the UAV can be extracted from the contents of the DJI GO application and used to track the specific device used in flight. The data reveals information about the UAV's internal system operations such as updates and errors. A log is also kept of times when the UAV encountered a no fly zone (NFZ) during flight. Media is present as copies of videos captured during flight are locally stored by the application. Flight data files with the ".txt" extension were extracted from the "FlightRecord" directory. The contents of these files will be discussed in the next section in comparison with the flight data extracted from the internal storage. These files possessed a number of useful metadata artefacts, which was viewed using

the "CsvView" application [16]. One of the artefacts was the serial number which matched that of the UAV, meaning the UAV is traceable in the event of capturing artefacts from a mobile platform.

TABLE IV. USEFUL DIRECTORIES FROM DJI GO APPLICATION

Path	Type	Description
/media/0/DJI/dji.pilot/LOG/CACHE	Flight Data	Contains a number of logs relating to drone activity
/media/0/DJI/dji.pilot/LOG/CACHE/NFZ	Flight Data	This is a log of activity relating to the DJI's built-in no fly zone function, and contains information such as GPS location.
/media/0/DJI/dji.pilot/LOG/ERROR_POP_LOG	Flight Data	An error log from the UAV.
/media/0/DJI/dji.pilot/DJI_RECORD	Media	A number of vide stored with the "mp4" file extension. For each video file, there is also a corresponding text file, which contains GPS data, manufacturing information and capture dates.
/media/0/DJI/dji.pilot/FlightRecord	Identifying Artefacts	Flight data relating to a number of flights. A string search of these files revealed the presence of the "cccu phantom" string, which was the name assigned to the UAV during setup, as well as the UAV serial number.
/media/0/DJI/dji.pilot/CACHE_IMAGE	Media	Thumbnails of various images and videos taken during flight.

2) A.R Drone 2.0

The "userdata/data/com.parrot.freeflight" directory contained several ".xml" files, with names in the format of "<MAC Address of mobile platform>_<Timestamp>". These appear to correlate with sessions of activity on the UAV. Each file contains a number of flight and application session records, with each XML (Extendable Markup Language) block being named accordingly. The "FLIGHT_DRONE_SERIAL" tag displays a matching serial number to the one extracted from the UAV, providing the same traceability as mentioned in the previous section. Another XML file, located in "userdata/com.parrot.freeflight/shared_prefs/Preferences.xml" held a number of important artefacts, including the GPS co-ordinates of the last flight, the email address of the google account used to download the application, and when the application was last opened. The A.R Freeflight application has a media storage location in the platform's "userdata/media/0/DCIM" (Digital Camera IMage) directory, which contains all the media captured by the UAV's cameras. EXIF data for these files varies, some containing GPS information which matches the operator location during the flight, and some only containing a few details such as the creation date.

B. *Flight Data*

Flight data was successfully recovered from both UAV platforms. In each case flight data was useful in re-constructing the actions taken by the drone and the operator and included numerous details such as flight paths and outputs from the operating system of the UAV. Flight data can also be correlated with artefacts recovered from the mobile platform and removable storage.

1) DJI Phantom 3 Professional

The files extracted from the internal storage of the DJI Phantom were analysed using the "CsvView" tool [16]. The DJI Phantom 3 Operating system begins recording flight data from the moment the UAV is switched on. This meant flights performed in the same session of drone activity were recorded in one file, "FLY012.DAT". After processing using "CsvView", which converts the file from a ".DAT" to a ".csv" format, the flights were visualised using the "GeoPlayer" function, which utilised the Google Maps API Key mentioned in part B of Section 3. This visualisation is shown in Figure 2, with each flight, waypoints 1-4 and the point of interest (POI) highlighted.

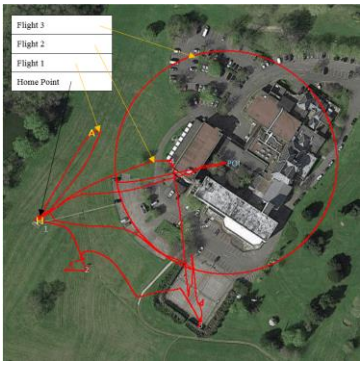

Fig. 2. Visualised GPS data

Other flight data extracted from the ".DAT" files included data streams from a host of on-board sensors. Plotting these streams against each other using "CsvView" allowed the drones actions to be deduced. Plotting the flight time (green), the barometric altitude (blue) and total battery voltage (purple) revealed three distinct periods of activity, which are interpreted as flights. The flight time increases linearly when the drone is in flight. This is shown in Figure 3.

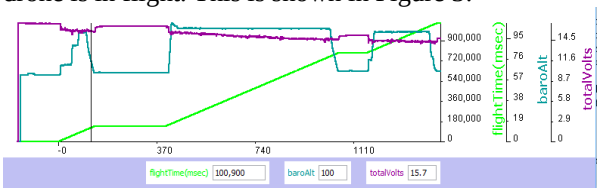

Fig. 3. Flight time, altitude and battery levels

The DJI Phantom logs provide an extensive amount of sensor data, including but not limited to acceleration, GPS health, and temperature. Collating these data streams can reveal a great deal about the actions taken by the UAV. The DJI GO flight logs mentioned in part A of Section 4 provided a similar set of streams, however there were less than the flight logs on the UAV and a lower resolution. The application logs also contained data available from the DJI GO application, such as whether the UAV was piloted in manual or automatic mode. A period of autonomous control state is

highlighted in green in Figure 4. During flight 3 (Figure 2), the drone performed an automatic POI function which made it fly in a circle around a pre-determined point. Examining "distance from home" stream from the application flight log for this flight reveals the function generates a clearly visible sine wave when executed, as shown in Figure 4. The presence of sine wave directly indicates the use of the POI function.

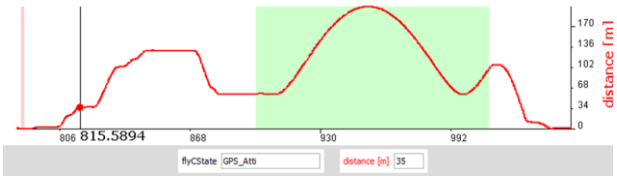

Fig. 4. Distance from home plotted against UAV flight state.

2) A.R Drone 2.0

The files copied from the internal storage of the A.R Drone 2.0 were analysed using scripts and utilities on the forensic workstation. A number of files of interest were located, listed in Table 5. As the internal system is based on Linux, some common locations for forensic artefacts were analysed such as the "syslog.bin" file which contains threads relating to software processes running on the drone system and the "config.ini" file which contains serial numbers, version numbers and the name assigned to the UAV. Some files specific to the A.R Drone were also analysed, with the "sessions" and "profiles" configuration files which correlate with artefacts found using mobile forensics techniques.

TABLE V. LIST OF FILES ACQUIRED FROM A.R DRONE

Path	Type	Description
/data/syslog.bin	System log, containing details of various software and hardware events from the UAV's internal operating system.	Version information, configuration data, mount information, file creation logs
/data/config.ini	Configuration file for the UAV.	Drone serial number, software version, drone name, access point SSID
/data/emergency.bin	Unidentified binary file. Further work should identify the importance of this file and it's cybersecurity implications.	n/a
/data/custom.configs/sessions/	Directory containing several files named "config.xxxxxxxx.ini"	GPS data. The UAV does not have a GPS sensor installed so it likely originated from the A.R Freeflight application.
/data/custom.configs/profiles/	Directory containing a file named "config.xxxxxxxx.ini".	Contains a footprint from the controlling application with name of the mobile platform, "Mororola_MotoG3" and a serial number – "PS721003AJ4K103341".

The "data/syslog.bin" was analysed using command line tools. Separate processes running on the A.R Drone leave named artefacts in the system log, and filtering these artefacts returned threads of activity. All threads containing the string "UsbKey" related to the removable storage device of the A.R Drone 2.0. Further filtering for the "Serial" string returned a history of the USB keys attached to the A.R Drone, as shown in Figure 5.

```
root@lab:~/drones/parrot/acquisition# cat syslog.bin | grep "UsbKey" | grep "Serial"
2.599151 UsbKeyMonitor 6  905   USB Mass Storage Serial    = '076511810BAC'
2.461425 UsbKeyMonitor 6  912   USB Mass Storage Serial    = '20020501A5BCF703'
2.464935 UsbKeyMonitor 6  915   USB Mass Storage Serial    = '20020501A5BCF703'
2.690795 UsbKeyMonitor 6  918   USB Mass Storage Serial    = '20020501A5BCF703'
2.463745 UsbKeyMonitor 6  914   USB Mass Storage Serial    = '20020501A5BCF703'
2.451904 UsbKeyMonitor 6  914   USB Mass Storage Serial    = '20020501A5BCF703'
2.657562 UsbKeyMonitor 6  910   USB Mass Storage Serial    = '0000177BE961C012'
2.453735 UsbKeyMonitor 6  898   USB Mass Storage Serial    = '078A01110998'
root@lab:~/drones/parrot/acquisition#
```

Fig. 5. USB key serial number history

Filtering the system log for all "UsbKeyWriter" outputs gave a history of all files created on the removable storage, with system times. Filtering for the "Video" outputs gives a log of the use of both the UAV's internal cameras, which video codec is being used and other details including resolution. Examination of the "syslog.bin" file give a comprehensive overview of actions carried out by the UAV's operating system. Values found also reflected values in the "config.ini" files listed in Table 5. Future work should identify whether modification of the "config.ini" files would change data in the system log, for anti-forensics purposes.

C. Media

To examine the EXIF data from the media captured by the drone, the command line "exiftool" [18] was used, as mentioned in part C of Section 3.

1) DJI Phantom 3 Professional

"Exiftool" was run against the DCIM/100MEDIA directory of the DJI Phantom's removable storage media. On initial inspection, GPS co-ordinates are stored under a "GPS Position" EXIF tag. To automate the process of extracting the GPS co-ordinates and create a timestamped GPS media log, a simple script was created, as shown in Figure 6.

```
exiftool * -c "%.6f %.6f %.6f" | egrep 'GPS Position|Create Date'
```

Fig. 6. Script to retrieve GPS data from media EXIF information

The script formats the GPS data to 6 decimal places. The output is then filtered to only contain the GPS Position and Create Date, which denotes when the picture or video was taken. The output of this script is seen in Figure 7. The output of this script could be used to create a visual map of all the photos taken during flight.

```
root@lab:/mnt/analysis/DCIM/100MEDIA# ~/drones/dji/script.sh
Create Date                     : 2017:04:01 14:07:30
GPS Position                    : 51.000000 15.000000 28.380300 N, 0.000000 36.000000 53.406800 E
Create Date                     : 2017:04:01 14:07:30
GPS Position                    : 51.000000 15.000000 28.380800 N, 0.000000 36.000000 53.412300 E
Create Date                     : 2017:04:01 14:07:46
Track Create Date               : 2017:04:01 14:07:46
Media Create Date               : 2017:04:01 14:07:46
GPS Position                    : 51.000000 15.000000 28.378800 N, 0.000000 36.000000 53.391600 E
Create Date                     : 2017:04:01 14:09:10
GPS Position                    : 51.000000 15.000000 27.342900 N, 0.000000 36.000000 54.332000 E
Create Date                     : 2017:04:01 14:09:10
GPS Position                    : 51.000000 15.000000 27.347600 N, 0.000000 36.000000 54.334400 E
```

Fig. 7. Output of GPS extractor script

2) A.R Drone 2.0

While photos taken by the A.R are actually stored by the A.R Freeflight application, any videos taken are stored on the removable storage. Examination of the video files using "exiftool" revealed a number of artefacts, including creation time and the device name "Parrot AR.Drone". The "ARDroneTelemetry" tag was extracted from one of the videos using the "-b" option. This returned a set of floating point numbers and integers, with no labels or column headers. Using heuristics based on knowledge of the drone system and flight data, it was deduced that the first of the floating points was a timestamp, as it increased in regular increments. Also deduced was that the last floating point was the altitude of the UAV during flight, as the values steadily changed, and matched the approximate value of the flight. The telemetry data was dumped to a file for analysis with the command "exiftool –b –ARDroneTelemetry media20170401_150213/video_20170401_150249.mp4 > ~/drones/parrot/gnuplot/telemetry". A bash script was created to convert the data to a comma-separated value file, which could then be visualised using the "gnuplot" [19] tool for Linux. The altitude was plotted over the period of the whole video, as seen in Figure 8.

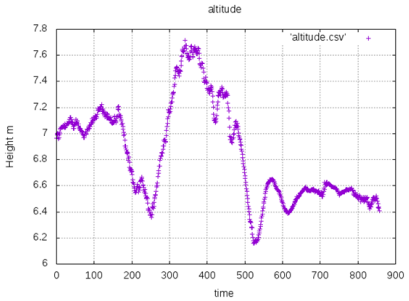

Fig. 8. Altitude measurements for the duration of an extracted video file

V. Conclusion

Analysis of data acquired from both drone platforms revealed operational differences between the DJI Phantom 3 Professional and the A.R Drone 2.0. However, a number of common methods were demonstrated to recover data from these multi-platform drone systems. In drone forensics, there is a wealth of valuable information available from analysis of the associated mobile platform used to control the UAV. Flight logs and identifying artefacts can often be found within the data of the respective controlling application. Analysis of flight data reveals actions taken by the UAV and can be useful in re-constructing flights that took place, which is useful for crimes such as smuggling mentioned in Section 1. This requires correlation of data streams from the sensors available on the UAV. Media captured by the drone also contains useful information, especially when geotagged such as the case of the DJI Phantom 3 Professional. The content of the media itself is also pivotal information when investigating crimes such as invasion of privacy. The forensic analysis of drones requires a polymathic style of work - simultaneously being able to adapt to the many embedded and mobile environments that may be encountered. Future work should focus on other mobile platforms not covered in the scope of this paper, including iOS and Windows Phone. Other popular drone platforms should also be analysed. The methods discussed in this paper can be integrated into commercial forensics toolkits to develop support for drone systems. This would highly benefit the digital forensics community in the emerging area of drone forensics.

References

[1] P. Yeung, "Drone reports to UK police soar 352% in a year amid urgent calls for regulation," The Independent, August 2016. Available on-line at http://www.independent.co.uk/news/uk/home-news/drones-police-crime-reports-uk-england-safety-surveillance-a7155076.html [Accessed May 2017]

[2] BBC news, "Big rise in drone smuggling incidents" February 2016. Available on-line: http://www.bbc.co.uk/news/uk-35641453 [Accessed May 2017]

[3] A. Noel, "Drone carrying three Kilos of Meth crashes in Tijuana," Vice News, January 2015. Available on-line: https://news.vice.com/article/drone-carrying-three-kilos-of-meth-crashes-in-tijuana [Accessed May 2017]

[4] CAA - "Flying Drones," Web page available on-line: https://www.caa.co.uk/Consumers/Guide-to-aviation/Airspace/Who-manages-UK-airspace-/ [Accessed May 2017]

[5] D. Barrett., "Burglars use drone helicopters to target homes," The Telegraph, May 2015. Available on-line: http://www.telegraph.co.uk/news/uknews/crime/11613568/Burglars-use-drone-helicopters-to-identify-targe-homes.html

[6] A. Glaser, "DJI is running away with the drone market," Recode, April 2017. Available on-line: https://www.recode.net/2017/4/14/14690576/drone-market-share-growth-charts-dji-forecast [Accessed May 2017]

[7] UAV Systems international – "Tarot T-18 Ready to Fly Drone," Available on-line: https://uavsystemsinternational.com/product/tarot-t-18-ready-fly-drone/ [Accessed May 2017]

[8] G. Horsman, 2016. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. Digital Investigation 16, 1–11.

[9] M. Maarse, L. Sangers, J. Ginkel, and M. Pouw, "Digital forensics on a DJI Phantom 2 Vision+ UAV," Thesis published 2016.

[10] F. Trujano, B. Chan, G. Beams, and R. Rivera, "Security Analysis of DJI Phantom 3 Standard," Massachusetts Institute of Technology, 2016.

[11] B. Carrier, 2002. "Open source digital forensics tools: The legal argument" pp. 1-11, Stake, 2002.

[12] CyanogenMod Custom Android Operating System - https://github.com/CyanogenMod [Accessed May 2017]

[13] T. Barton, and M. H. B. Azhar, "Forensic analysis of the recovery of Wickr's ephemeral data on Android platforms," The First International Conference on Cyber-Technologies and Cyber-Systems, IARIA, pp. 35-40, 2016.

[14] Android Debug Bridge tool for windows and Linux - https://developer.android.com/studio/command-line/adb.html [Accessed May 2017]

[15] D. Kovar, "UAV (aka drone) Forensics," SANS DFIR Summit, 2016.

[16] CsvView tool - https://datfile.net/CsvView/downloads.html [Accessed May 2017]

[17] Nmap tool for Linux and Windows - https://nmap.org/ [Accessed May 2017]

[18] Exiftool for Linux - http://www.sno.phy.queensu.ca/~phil/exiftool/ [Accessed May 2017]

[19] Gnuplot for Linux - http://www.gnuplot.info/ [Accessed May 2017]