Challenges and Techniques in Drone Forensics

Dr Hannan Azhar
Canterbury Christ Church University
School of Engineering, Technology and Design
hannan.azhar@canterbury.ac.uk

NexTech 2019,
22 Sept, Porto, Portugal
Commercial Drones are Taking Off
Projected worldwide market growth for commercial drones

- Revenue (in billion U.S. dollars)
  - 0.6
  - 0.8
  - 1.1
  - 1.6
  - 2.4
  - 3.6
  - 5.3
  - 7.6
  - 10.1
  - 12.6

- Drones sold (in thousands)
  - 110
  - 159
  - 246
  - 392
  - 634
  - 996
  - 1,414
  - 1,909
  - 2,329
  - 2,679

Source: Tractica

Dr Hannan Azhar@ NexTech2019, Porto, Portugal
Worldwide drone incident

https://www.dedrone.com/resources/incidents/all
Drone Related Crimes

Britain is facing an explosion in drone crimes, with reported incidents now numbering more than six a day - a rise of 45 per cent in three years. From 1,518 in 2016 to 2,204 in 2018 - Daily Mail 17 May 2019

63 reports involving playgrounds and nurseries in eight police force areas alone between 2016 and 2018

Drones appearing to follow children in parks, playgrounds, swimming pools and even children’s homes.

Burglars use drone helicopters to target homes

Flights from Gatwick Airport were suspended after multiple drones were deliberately flown over the airfield. Sussex Police has spent more than £400,000 investigating the case, but no one was found.

Endless crimes from assassinations, terrorist attacks, simple theft or deliberate economic disruption

Dr Hannan Azhar@ NexTech2019, Porto, Portugal
Prison delivery

https://www.youtube.com/watch?v=3zXq7ywyCnY
Reported crimes

- Harassment,
- Stalking,
- Burglary,
- Drugs, supply to prisons
- Smuggling
- Voyeurism
- Airport Drone Chaos
- Warfare
- spy military installations and sensitive institutions

**Mexican cartels are turning to drones to smuggle lightweight drugs like heroin and cocaine over the U.S. border rather than using tunnels.** *(Associated press)*

Capture the drone

https://www.youtube.com/watch?v=rah_i7FFGRw
Identify Drones

- According to FAA (Federal Aviation Administration)
- There are over 1.3 million registered drones owners in USA;
- 116,000 registered drone operators;
- Hundreds of thousands are not registered;
- 7 million will fly over USA by 2020;
- Small drones to display registration numbers on the exterior to address concerns raised by U.S. security officials and to make it easier to identify owners.

https://www.reuters.com/article/us-usa-drones/u-s-agency-requires-drones-to-list-id-number-on-exterior-idUSKCN1Q12O9
Drones are multi-platform systems

A drone system consists of:
- Controller, Mobile phone, Camera, The Drone itself, Cloud
- Questions to ask?
  - Where data is located?
  - What kind of data is accessed?
  - What is the process?
    - Forensics Soundness
    - Extraction level (e.g. device Intact? Logical? Physical? Chip off? Cloud?)
Admissibility to Court

- ACPO (Association of Chief Police Officers) principles:
  - Principle 1: The data held on an exhibit must not be changed.
  - Principle 2: Any person accessing the exhibit must be competent to do so and explain the relevance and the implications of their actions.
  - Principle 3: A record of all processes applied to an exhibit should be kept. This record must be repeatable to an independent third party.
  - Principle 4: The person in charge of the investigation has responsibility for ensuring that the law and these principles are adhered to.

- Justification for our actions
- Repeatability
- A full understanding of the implications of any actions taken

Extraction Level from Device

Source: Sam Brothers, "Cell Phone and GPS Forensic Tool Classification System", 2009
Drone Cloud forensics challenges

- Multi-tenancy challenges
  - Shared Memory access
  - Violation of confidentiality and privacy agreement
- LEA can only exercise power within their authorised jurisdictions
- The Acquisition and Disclosure of Communications Data - Regulation of Investigatory Powers Act 2000 governs UK LEAs’ powers to acquire data.
- Although DFEs can technically acquire data from a cloud server in a foreign country using a suspect’s device via a connection with that server,
- They may breach laws in that jurisdiction because UK courts cannot authorise such action in foreign countries.

Drone Artefacts

- Information on its owner
- Flight paths, launch location and landing destination
- Photos and videos that enables investigators to pinpoint suspect.
- Serial number that can be used to trace the owner
- Version numbers for firmware
- Information on change of state: launch/land, manual/waypoint operation and GPS available/unavailable
- Geo-location information for launch, land and home point locations
Drone Forensics Framework

Step 1: Identify the chain of command
Step 2: Allow conventional forensics to examine the U.A.S
Step 3: Identify the role of the U.A.S in the crime.
Step 4: Photograph the U.A.S
Step 5: Identify make and model through visual inspection looking for serial numbers and other markings.
Step 6: Open source research into device. Look for available tools and information relating to the drone.
Step 7: Identify the drone capabilities, audio/visual recording, carrying capacity, etc.
Step 8: Identify modifications
Step 9: Identify data storage locations
Step 10: Search for ways to extract data from the drone
Step 11: Extract removable storage mediums
Step 12: Create a forensic copy
Step 13: Perform traditional interrogation of extracted data
Step 14: Use non-traditional methods e.g. open source tools
Step 15: Live forensics
Step 16: Interrogation of peripherals
Step 17: Destructive forensic techniques (if required)
Step 18: Review extracted data.
Step 19: Find case relevant data
Step 20: Create report.

Unmanned Aerial Vehicle Forensic Investigation Process: Dji Phantom 3 Drone As A Case Study
Roder et al. 2018

Forensic Approach- Case studies

- We used a model for forensic research based on experience in previous projects

Preliminary Research
- Establish use of technology in crime
- Establish capabilities of technology
- Estimate methodology

Scenario Creation
- Simulate crime scenario
- Utilise technology to its full potential
- Gather data

Data Acquisition
- Finalise methodology
- Acquire data in a forensically sound method (ACPO)

Data Analysis
- Highlight important artefacts
- Filter out non-useful data

Report and Present
- Preserve method
- Ensure repeatability

Association of Chief Police Officers (ACPO)
Drone Forensics- Case studies

- We will focussed on two different drones; the DJI Phantom 3 Professional and the Parrot A.R 2.0 Power edition
- Phantom highly capable device with an array of sensors and on-board processing power, used for photography, surveying and recreation

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifications</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>DJI Phantom 3 Professional</td>
<td>Weight: 1280g, Camera Resolution: 4K (12 Megapixels)</td>
<td>5Km</td>
</tr>
<tr>
<td>A.R Drone 2.0</td>
<td>Weight: 380g / 420g, Camera Resolution: 720p (0.9 Megapixels)</td>
<td>50m</td>
</tr>
</tbody>
</table>
Phantom 3 Pro Artefacts

DJI GO Application
- Personally Identifiable Information
- Flight Data Logs (GPS, Speed, Battery Level)
- Captured Media
- Serial Number

Acquisition method: Mobile forensics
- Flight Data (Temporal)
- Serial Number
- Acquisition method: access via network

16 gb microsd card - removable a micro SD card, glued on to the centre board

DJI Phantom 3 Professional UAV
- Controller Footprint
- Captured Media
- Serial Number
- Pairing Information

Acquisition method: Imaging removable media and internal storage

Dr Hannan Azhar@ NexTech2019, Porto, Portugal
A.R. Drone 2 Artefacts

A.R Freeflight Application
- Personally Identifiable Information
- Flight Data Logs (Accelerometer, Battery Level, Ultrasonic Altimeter)
- Captured Media
- Serial Number

Acquisition method: Mobile forensics

2.4 GHz Wi-Fi

32GB SD card, external

A.R Drone 2.0 UAV
- Controller Footprint
- Captured Media
- Serial Number

Acquisition method: Imaging removable media, access via network
Methodology

- A range of digital forensics methods were utilised:

<table>
<thead>
<tr>
<th>Component</th>
<th>Forensic Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling application(s)</td>
<td>Android Forensics</td>
</tr>
<tr>
<td>Drone</td>
<td>Linux Forensics</td>
</tr>
<tr>
<td>Controller</td>
<td>Network Forensics</td>
</tr>
<tr>
<td>SD Card, Internal storage</td>
<td>Standard digital storage method</td>
</tr>
<tr>
<td>Cloud storage</td>
<td>Cloud forensics</td>
</tr>
</tbody>
</table>

- The objectives of forensic analysis are to firstly find out the actions taken by the drone, link the drone to it’s controlling applications and then trace the system to a user with personally identifiable artefacts.

- Acquisition and Disclosure of Communications Data - Regulation of Investigatory Powers Act governs UK LEAs’ powers to acquire data- UK court may not authorise data acquisition from a server in a foreign country.
Scenario Creation (Urban environment)

- Before analysis, data needed to be gathered by flying the Phantom in a suitable site;
- Large open space
- Tall building structures
- Several distinct waypoints within the site
Scenario creation cont.

<table>
<thead>
<tr>
<th>Flight</th>
<th>Start Time</th>
<th>Waypoints</th>
<th>End Time</th>
<th>Description, Notes and Recorded Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13:17</td>
<td>Travelled a short distance north of the Home Point before returning.</td>
<td>13:18</td>
<td>Test flight for compass calibration</td>
</tr>
<tr>
<td>3</td>
<td>14:17</td>
<td>Automatic Reconnaissance Flight Auto Land (Return to home) 14:22</td>
<td>14:22</td>
<td>Automatic Flight, GPS Assisted. Using DJI’s built-in Point Of Interest (POI) function, which makes the drone rotate around a specified point. Video was recorded the entire flight.</td>
</tr>
<tr>
<td>4</td>
<td>14:34</td>
<td>(Same waypoints at Flight 2, time not recorded due to operator concentrating on flight) Manual Landing</td>
<td>14:37</td>
<td>In this flight, foil was attached to the drone covering the GPS module. The drone was operated completely manually independent of GPS. This simulated the intentional obfuscation of GPS signals as mentioned in related work [15] [16].</td>
</tr>
</tbody>
</table>

Phantom 3 Data Acquisition

- Connected directly to forensic workstation, forensic image created using DD tool.
- SD card, FAT32

Phantom put in data mode through DJI GO app

- Connected to forensic workstation using USB cable, forensic image created using DD tool (very slow!)
- "FLY012.DAT"

- GPS data

Dr Hannan Azhar @ NexTech2019, Porto, Portugal
After rooting, listing the "ls /dev/block/bootdevice/by-name" directory gives list of partitions.

Forensic bit-for-bit image created on micro SD card using dd tool.
Results - SD Card (External)-Phantom
“tree” - Open source Linux utility

- Preliminary assessment to test contents of SD card
- Tree command used to list all active files and give general idea of directory structure
- Results show external SD card used to store mostly media files in .JPG, .DNG and .MP4 format
Results - SD Card (External) - Phantom

“exiftool” - Open source Linux utility

- Artefacts can be extracted from the EXIF (Exchangeable Image File) data of the photo and video files
- To automate this process, the Linux tool “exiftool” was run against the whole media directory and “egrep” used to filter the results
- In this case only the GPS co-ordinates and the create date were selected but there are many more that could be included
Results - Internal SD Card-(Phantom)

- The internal storage of the Phantom contains a number of flight logs - one per session of activity (power on to power off) so one log may contain multiple flights
- The logs are stored in a format with a “.DAT” extension
- They were analysed using the “CsvView” tool running on a windows machine
Results - Internal Storage (Cont.)

“CsvView” - Open Source Windows Toolkit

► “CsvView” offers 2 main features
  ► Read data streams from “.DAT” files and converts to “.csv”
  ► Geographic graphing of GPS co-ordinates (Seen on the right)
► Both were used to visualise the actions taken by the phantom during flight
► There are a host of data streams including but not limited to:
  ► Battery levels
  ► Internal temperature
  ► Barometric altitude
  ► Velocity and accelerometer readings
► “CsvView” allows these to be graphed against each other

“GeoPlayer” function in CsvView, which utilised the Google Maps API Key
Results - Internal Storage (Cont.)

- Flight time (green), Barometric Altitude (teal) and Total Voltage (purple) give a good idea of flight activity.

- Flight time increases in a linear fashion whenever the drone is in flight, barometric altitude indicates how high the drone was flown.

- X axis is an arbitrary measurement of how many samples were recorded in the log.
Results - Internal SD Card (Anti-forensics)

“CsvView” - Open Source Windows Toolkit

- Flight time (green) against Number of Satellites (red) shows how many GPS satellites the drone is connected to.

  ![Graph showing flight time against number of satellites]

- As part of our experiment we obscured the GPS unit with foil as an anti-forensics test.

- This is clearly visible in the above graph, where the number of satellites drops to 0 before flight commences.

Dr Hannan Azhar @ NexTech2019, Porto, Portugal
Results - Mobile Forensics - Phantom

- A wealth of artefacts were recovered from the data directory of the “DJI GO” android application
- These corroborated artefacts recovered from the UAV:
  - No fly zone log indicates when drone has attempted to breach an NFZ such as stadium or military base
  - Error logs
  - Media files with GPS co-ordinates
  - Flight records, similar to the “.DAT” logs discussed earlier
<table>
<thead>
<tr>
<th>Path</th>
<th>Type of Artefact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/media/0/DJI/dji.pilot/LOG/CACHE</td>
<td>Flight Data</td>
<td>Contains a number of logs relating to drone activity</td>
</tr>
<tr>
<td>/media/0/DJI/dji.pilot/LOG/CACHE/NFZ</td>
<td>Flight Data</td>
<td>This is a log of activity relating to the DJI’s built-in no fly zone function, and contains information such as GPS location.</td>
</tr>
<tr>
<td>/media/0/DJI/dji.pilot/LOG/ERROR_POP_LOG</td>
<td>Flight Data</td>
<td>An error log from the UAV.</td>
</tr>
<tr>
<td>/media/0/DJI/dji.pilot/DJI_RECORD</td>
<td>Media</td>
<td>A number of video taken during flight named as a date in the format “YYYY-MM-DD hh:mm:ss” and 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.</td>
</tr>
<tr>
<td>/media/0/DJI/dji.pilot/FlightRecord</td>
<td>Flight Data, Personally identifying information, UAV serial number</td>
<td>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.</td>
</tr>
<tr>
<td>/media/0/DJI/dji.pilot/CACHE_IMAGE</td>
<td>Media</td>
<td>Thumbnails of various images and videos taken during flight, seemingly random.</td>
</tr>
</tbody>
</table>
Results - Mobile Forensics (Cont.)

“CsvView” - Open Source Windows Toolkit

- The flight logs from the “DJI GO” application can also be visualised using “CsvView”, but with a few notable differences
  - Logs exist per-flight, rather than per session
  - Lower resolution data capture
  - Some application specific streams now available
  - Less sensor streams from the drone
- These logs give a detailed view of the actions the operator is taking while using the drone
Results - Mobile Forensics (Cont.)

“CsvView” - Open Source Windows Toolkit

- Metadata is available in “.TXT” logs which shows the serial number of the drone, allowing the pool of suspect devices to be reduced

<table>
<thead>
<tr>
<th>droneType</th>
<th>P3 Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>dateTime</td>
<td>2017/04/01 12:59:44.964</td>
</tr>
<tr>
<td>appVersion</td>
<td>3.1.4</td>
</tr>
<tr>
<td>batterySN</td>
<td>1589</td>
</tr>
<tr>
<td>aircraftSn</td>
<td>03Z1013321</td>
</tr>
<tr>
<td>appType</td>
<td>Android</td>
</tr>
</tbody>
</table>

- Serial number can be extracted from the hull of the aircraft
- This is a useful link from phone to drone
32GB SD card, FAT32

Connected to forensic workstation by 2.4 GHz WiFi

Connected directly to forensic workstation, forensic image created using DD tool.

Starting Nmap 7.12 ( https://nmap.org ) at 2017-03-26 18:15 BST
mass_dns: warning: Unable to determine any DNS servers, Reverse Nmap scan report for 192.168.1.1
Host is up (0.0094s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
5555/tcp open  freeciv
MAC Address: 90:03:87:92:53:38 (Parrot)

Controlling board running embedded Linux v2.6.32.9 with mounted Unsorted Block Image (UBI) file system

UBI has no block interface, so cannot be imaged directly, so files were logically copied to an SD Card
Upon connection the telnet welcome message identified as running "busybox" version 1.14.0

Running the "uname -r" command showed the UAV was running Linux version 2.6.32, which was released in 2009 (Kernel, 2009)

The amount of data present in the system log located at "/data/syslog.bin"

"cat syslog.bin | grep UsbKey" 

"UsbKeyMonitor" prints the serial number when a new USB device is attached, so filtering using the word "Serial" produced a history of all the USB keys attached to the UAV

Examination of the "syslog. bin" file give a comprehensive overview of actions carried out by the UAV’s OS
## Results - A.R Drone 2.0 Power Edition

### Internal Storage

**List of files acquired from A.R Drone 2.0 Internal Storage**

<table>
<thead>
<tr>
<th>Path</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/data/syslog.bin</td>
<td>System log, containing details of various software and hardware events from the UAV’s internal operating system.</td>
<td>Version information, configuration data, mount information, file creation logs</td>
</tr>
<tr>
<td>/data/config.ini</td>
<td>Configuration file for the UAV.</td>
<td>Drone serial number, software version, drone name, access point SSID</td>
</tr>
<tr>
<td>/data/emergency.bin</td>
<td>Unidentified binary file. Further work should identify the importance of this file and its cybersecurity implications.</td>
<td>n/a</td>
</tr>
<tr>
<td>/data/custom.configs/sessions/</td>
<td>Directory containing several files named “config.xxxxxxxxx.ini”</td>
<td>GPS data. The UAV does not have a GPS sensor installed so it likely originated from the A.R Freeflight application.</td>
</tr>
<tr>
<td>/data/custom.configs/profiles/</td>
<td>Directory containing a file named “config.xxxxxxxxx.ini.”</td>
<td>Contains a footprint from the controlling application with name of the mobile platform, “Motorola_MotoG3” and a serial number – “PS721003AJ4K103341.”</td>
</tr>
</tbody>
</table>
Results - A.R Drone 2.0 Power Edition
Mobile Forensics (A.R Freeflight application)

- "xml" files that correlate with sessions of activity on the UAV, containing serial number in the format of "< MAC Address of mobile platform> < Timestamp> ."
- The "FLIGHT_DRONE_SERIAL" tag displays a matching serial number which links phone to UAV
- Preferences file with GPS Co-ordinates of last flight (generated by phone)
- Another XML file, located in "userdata/com.parrot.freeflight/shared_prefs/Preferences.xml" finds GPS coordinates of the last flight, the email address of the google account used to download the application, and when the application was last opened.
- "Userdata/media/0/DCIM" (Digital Camera IMage) directory, which contains all the media captured by the UAV's cameras, GPS reading originated from mobile as this drone does not possess GPS
Results - A.R Drone 2.0 Power Edition
External Storage (32GB SD Card)

- The videos extracted from the external storage (USB stick) of the A.R Drone 2.0 were analysed and found to contain some interesting EXIF data.
- 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"
- Script was created to convert the data to a comma-separated value file, which could then be visualised using the "gnuplot" tool for Linux.

Altitude measurements for the duration of the extracted video file.
Dr Hannan Azhar@ NexTech2019, Porto, Portugal
SD Card using FTK
Oxygen forensics was only able to recover images and video from the apple phone backup of DJI Mavic

Others: Cellebrite ‘s UFED Physical analyser ; XRY Drone from MSAB
As of March 13 2019, it’s illegal to fly a drone within 5km of an airport. Rectangular extensions from the end of runways measuring 5km long by 1km wide to better protect take-off and landing paths.
UK FRZ map

FRZ = Flight Restricted Zone

https://dronesafe.uk/restrictions/

Dr Hannan Azhar@ NexTech2019, Porto, Portugal
Changes to Drone Legislation

- Since July 2018, new law bans drones flying anywhere in the UK above 400ft (122m), Or face a fine of up to £2500 or up to five years in prison.

- From November 30 2019,
  - Drone operators will have to register their device with the Civil Aviation Authority (CAA) and
  - Once registered the operator will receive a unique code that must be applied to all the drones they are responsible for
  - Take an online safety test (more details on this in the section below). This is also a legal requirement from the end of November for anyone flying a drone, whether or not they are a drone owner. There will be no charge for this
  - Anyone who fails to register or sit the competency tests could face fines of up to £1000

- [https://www.caa.co.uk/Consumers/Unmanned-aircraft/Our-role/Updates-about-drones/](https://www.caa.co.uk/Consumers/Unmanned-aircraft/Our-role/Updates-about-drones/)
- [http://publicapps.caa.co.uk/docs/33/CAP1763%20New%20UAS%20guidance%20Feb%202019.pdf](http://publicapps.caa.co.uk/docs/33/CAP1763%20New%20UAS%20guidance%20Feb%202019.pdf)
Thank you for listening

Any questions?

Dr Hannan Azhar
School of Engineering, Technology and Design
Canterbury Christ Church University
Canterbury, UK
hannan.azhar@canterbury.ac.uk

Read more:
