Challenges and Techniques in Drone Forensics

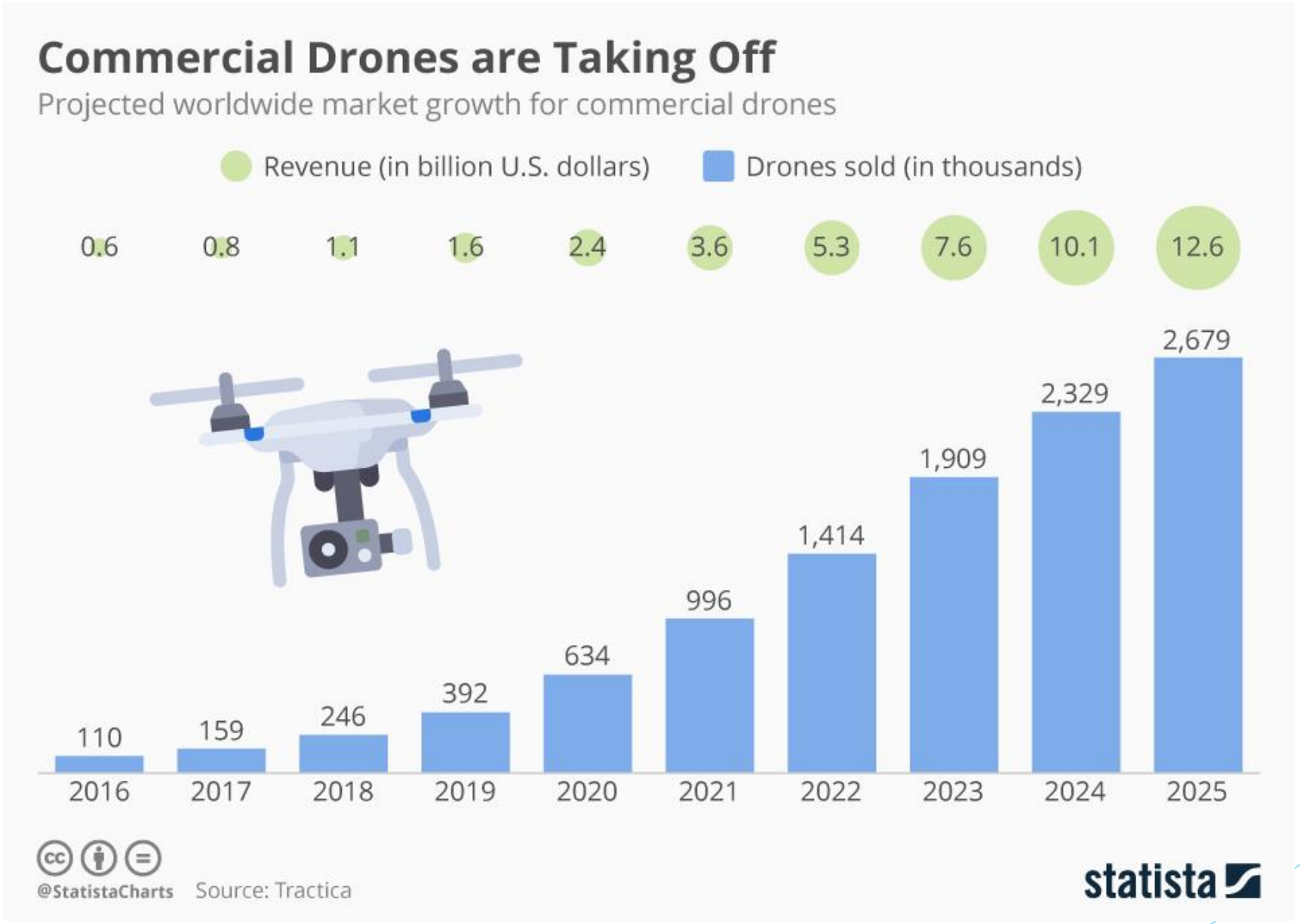
Dr Hannan Azhar

Canterbury Christ Church University

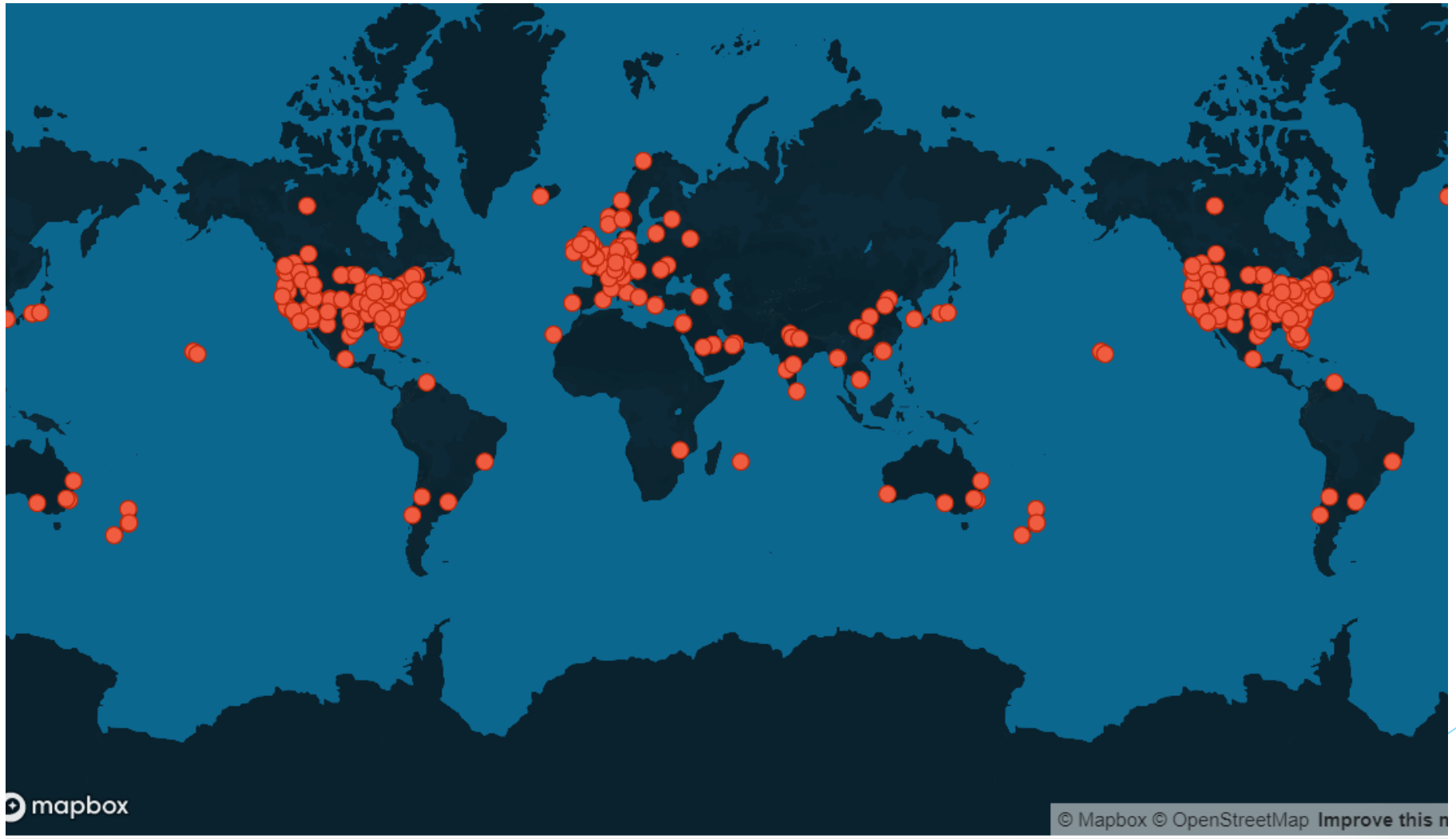
School of Engineering, Technology and Design

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)
Drones sold (in thousands)
0.6
0.8
1.1
1.6
2.4
3.6
5.3
7.6
10.1
12.6
110
159
246
392
634
996
1,414
1,909
2,329
2,679
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
@StatistaCharts
Source: Tractica
statista

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

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)

https://www.washingtontimes.com/news/2017/aug/20/mexican-drug-cartels-using-drones-to-smuggle-heroi/

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.nextgov.com/emerging-tech/2018/01/1-million-drones-operators-register-fly-us/145440/
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

Source: ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence for Digital Evidence March 2012 https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

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.

Source:
http://www.legislation.gov.uk/ukpga/2000/23/contents

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.

Preparation

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)

Examination

Step 18: Review extracted data.
Step 19: find case relevant data
Step 20: create report.

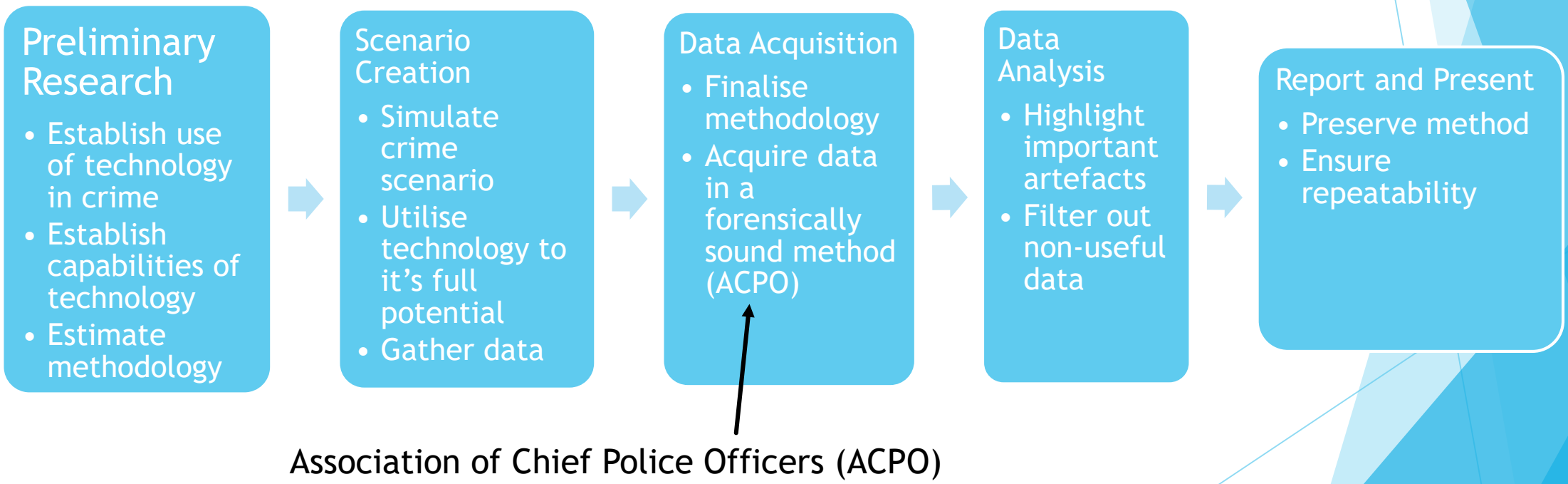
Report

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

https://arxiv.org/ftp/arxiv/papers/1804/1804.08649.pdf

Forensic Approach- Case studies

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



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

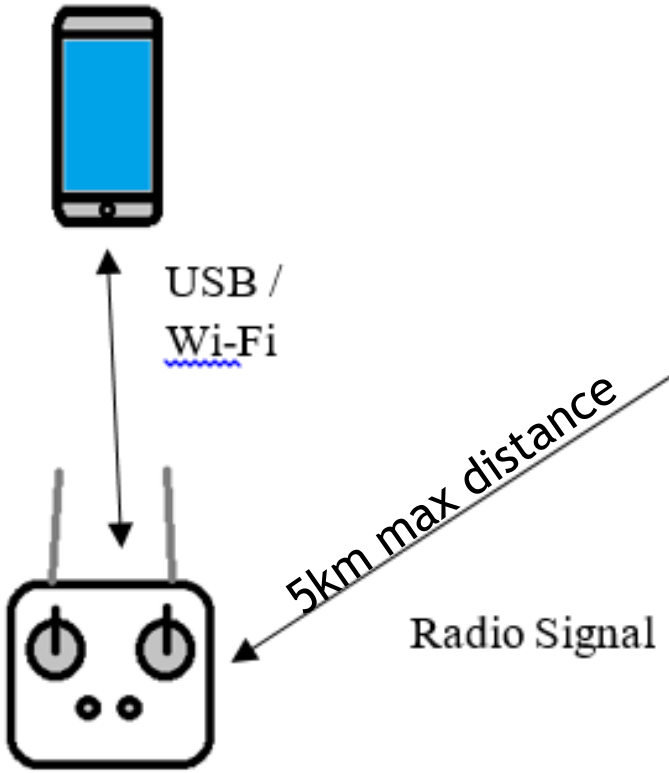
Name	Specifications		
	Weight	Camera Resolution	Range
DJI Phantom 3 Professional	1280g	4K (12 Megapixels)	5Km
A.R Drone 2.0	380g / 420g	720p (0.9 Megapixels)	50m

Phantom 3 Pro Artefacts

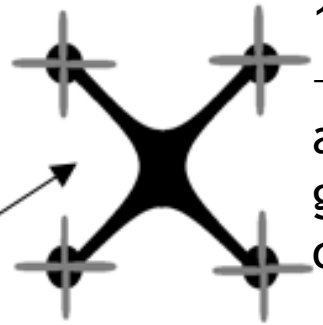
DJI GO Application

- 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



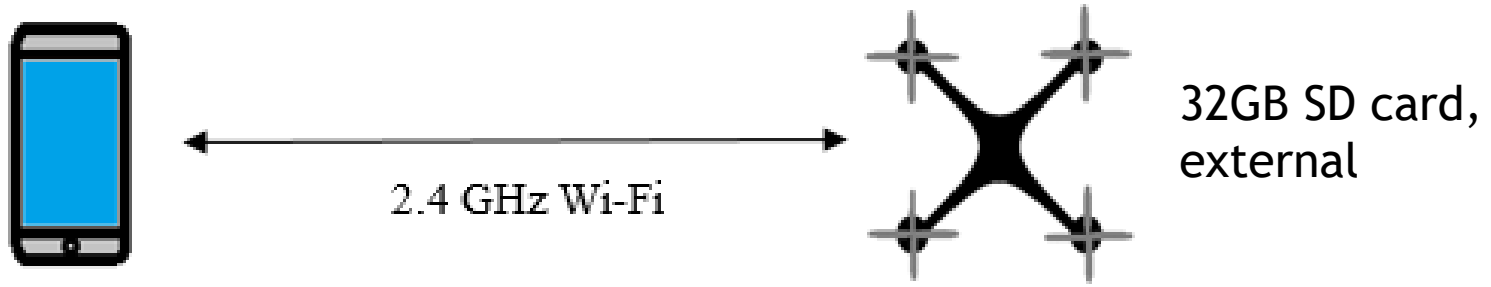
16 gb microsd card -removable
a micro SD card, glued on to the centre board

DJI Phantom 3 Professional UAV

- Controller Footprint
- Captured Media
- Serial Number
- Pairing Information

Acquisition method: Imaging removable media and internal storage

A.R. Drone 2 Artefacts



32GB SD card, external

A.R Freeflight Application

- Personally Identifiable Information
- Flight Data Logs (Accelerometer, Battery Level, Ultrasonic Altimeter)
- Captured Media
- Serial Number

Acquisition method: Mobile forensics

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:

Component	Forensic Method
Controlling application(s)	Android Forensics
Drone	Linux Forensics
Controller	Network Forensics
SD Card, Internal storage	Standard digital storage method
Cloud storage	Cloud forensics

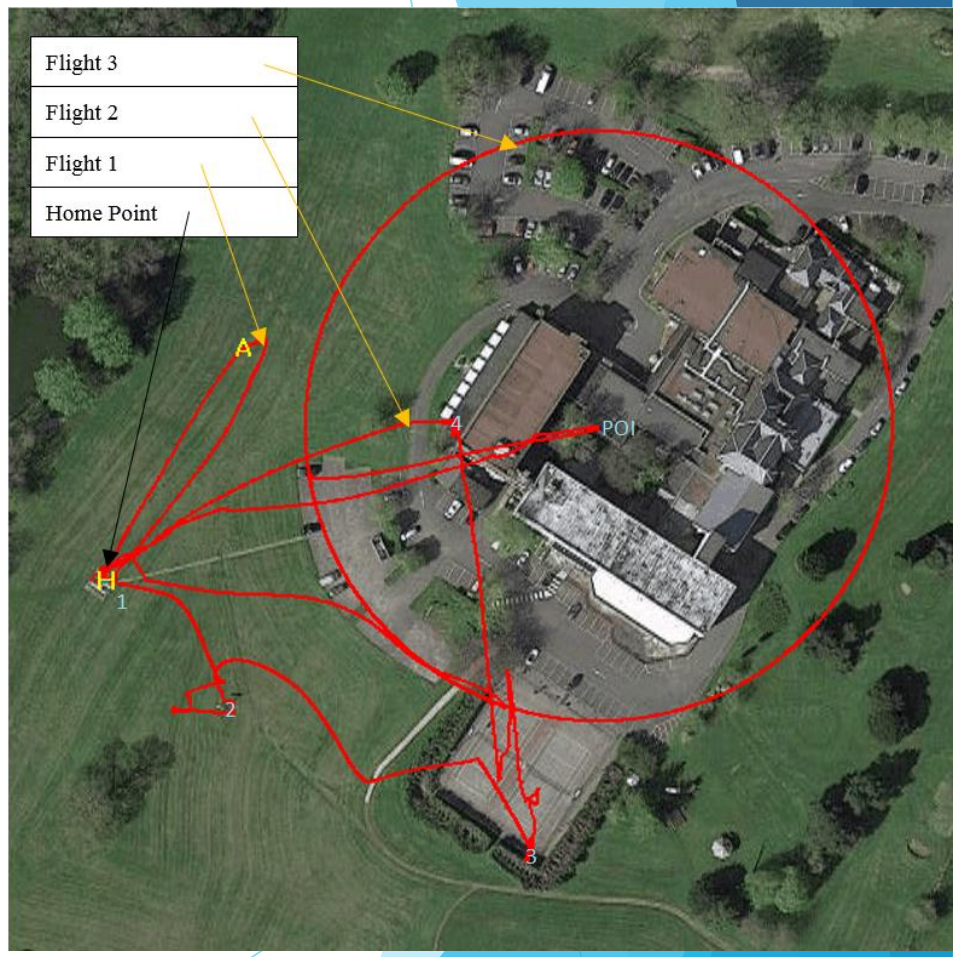
- The objectives of forensic analysis are to firstly find out the actions taken by the drone, link the drone to it's controlling applications and then trace the system to a user with personally identifiable artefacts
- Acquisition and Disclosure of Communications Data - Regulation of Investigatory Powers 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.*

Flight	Start Time	Waypoints	End Time	Description, Notes and Recorded Media
1	13:17	Travelled a short distance north of the Home Point before returning.	13:18	Test flight for compass calibration
2	14:05	Waypoint 1: 14:06 Waypoint 2: 14:07 Waypoint 3: 14:12 Waypoint 4: 14:14	14:15	Manual flight, GPS assisted, 1 photo and one short video taken at each waypoint.
3	14:17	Automatic Reconnaissance Flight Auto Land (Return to home) 14:22	14:22	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.
4	14:34	(Same waypoints at Flight 2, time not recorded due to operator concentrating on flight) Manual Landing	14:37	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].



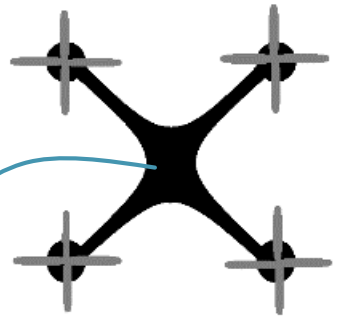
https://www.bbc.com/news/world-middle-east-46822429

Phantom 3 Data Acquisition

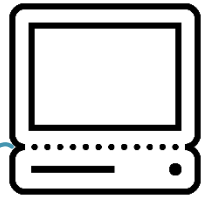
SD card, FAT32

GPS data

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

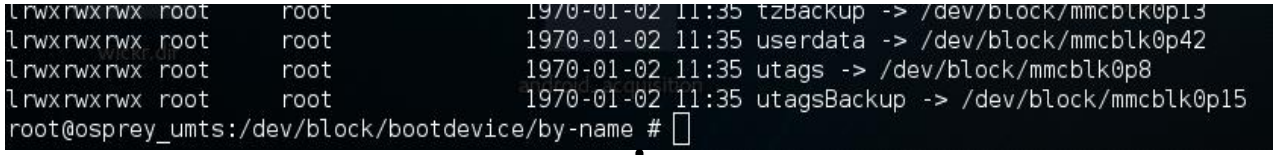


Phantom put in data mode through DJI GO app



Connected to forensic workstation using USB cable, forensic image created using DD tool (very slow!)

Mobile Forensics Data Acquisition



After rooting, listing the "ls /dev/block/bootdevice/by-name" directory gives list of partitions

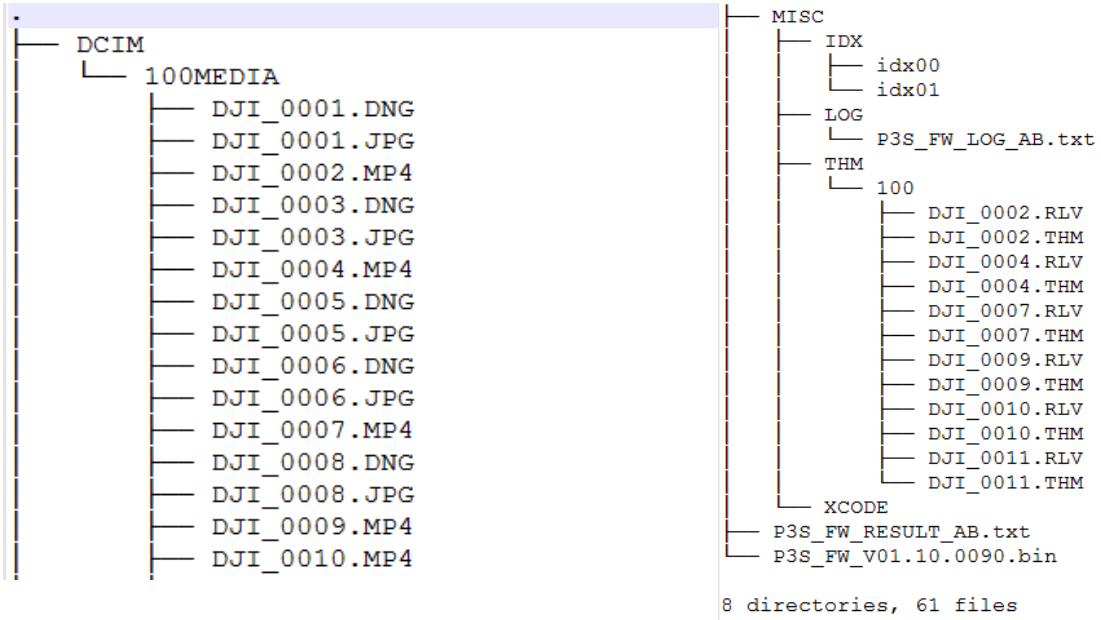
Forensic bit-for-bit image created on micro SD card using dd tool

Image mounted to forensic workstation

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

```
 GNU nano 2.5.3                                File: /root/drones/d

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

```
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
```

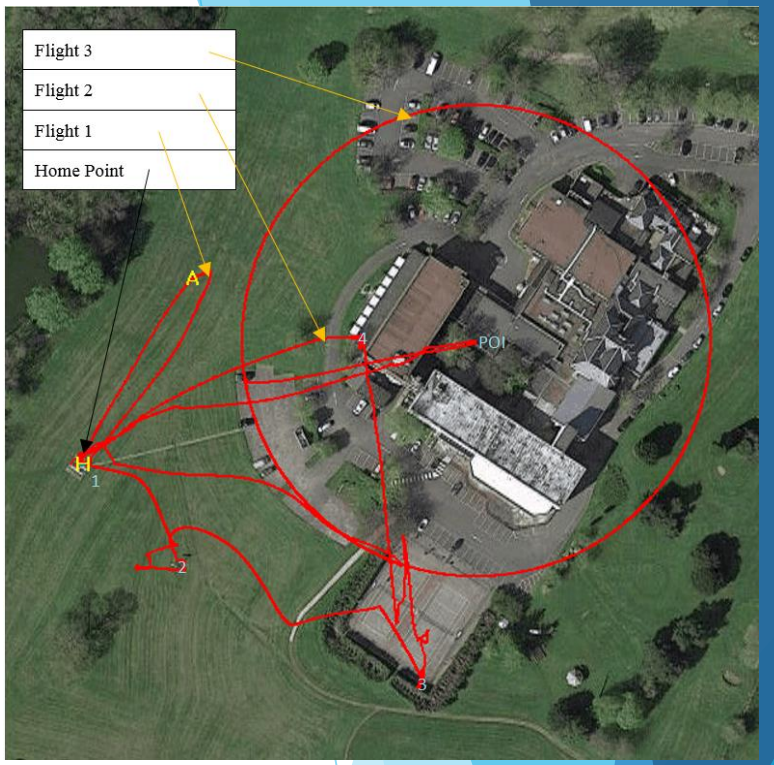
Results – Internal SD Card-(Phantom)

- 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

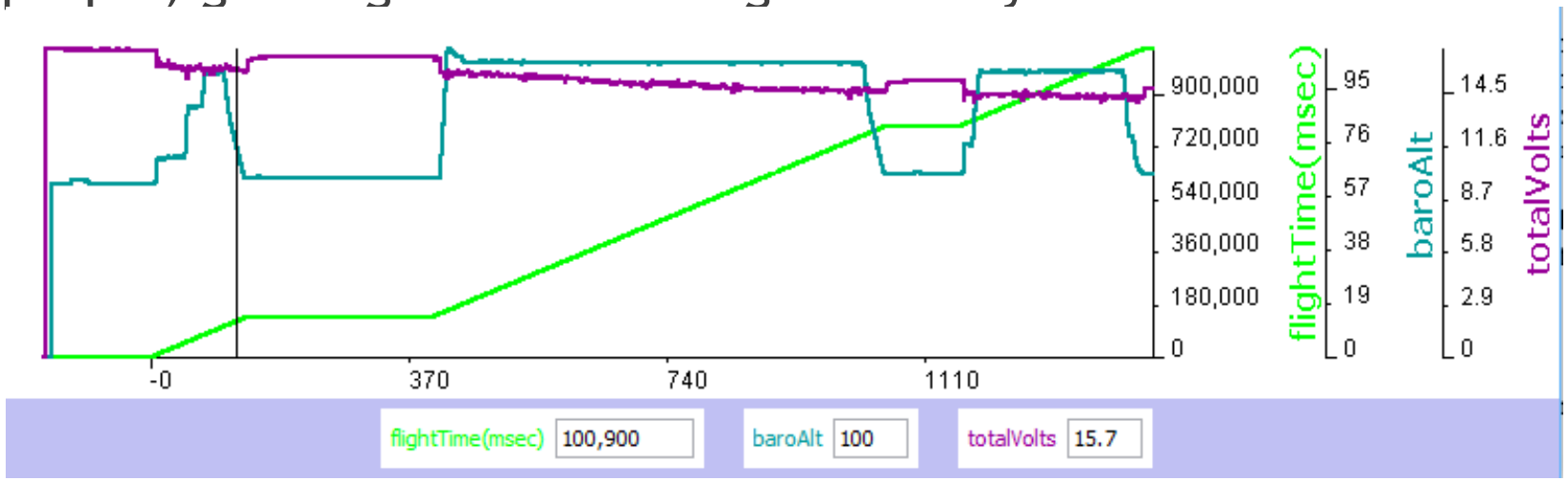
- "CsvView" offers 2 main features
  - Read data streams from ".DAT" files and converts to ".csv"
  - Geographic graphing of GPS co-ordinates (Seen on the right)
- Both were used to visualise the actions taken by the phantom during flight
- There are a host of data streams including but not limited to:
  - 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

- 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

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

DJI Go Artefacts

Path	Type of Artefact	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 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.
/media/0/DJI/dji.pilot /FlightRecord	Flight Data, Personally identifying information, UAV serial number	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.
/media/0/DJI/dji.pilot /CACHE_IMAGE	Media	Thumbnails of various images and videos taken during flight, seemingly random.

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

droneType	P3 Advanced
dateTime	2017/04/01 12:59:44.964
appVersion	3.1.4
batterySN	1589
aircraftSn	03Z1013321
appType	Android

- Serial number can be extracted from the hull of the aircraft
- This is a useful link from phone to drone

Parrot A.R Drone 2.0 Data Acquisition

32GB SD card, FAT32

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

Connected to forensic workstation by 2.4 GHz WiFi

```
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:B7:92:53:38 (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

```
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#
```

- 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 I 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

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."

Results – A.R Drone 2.0 Power Edition

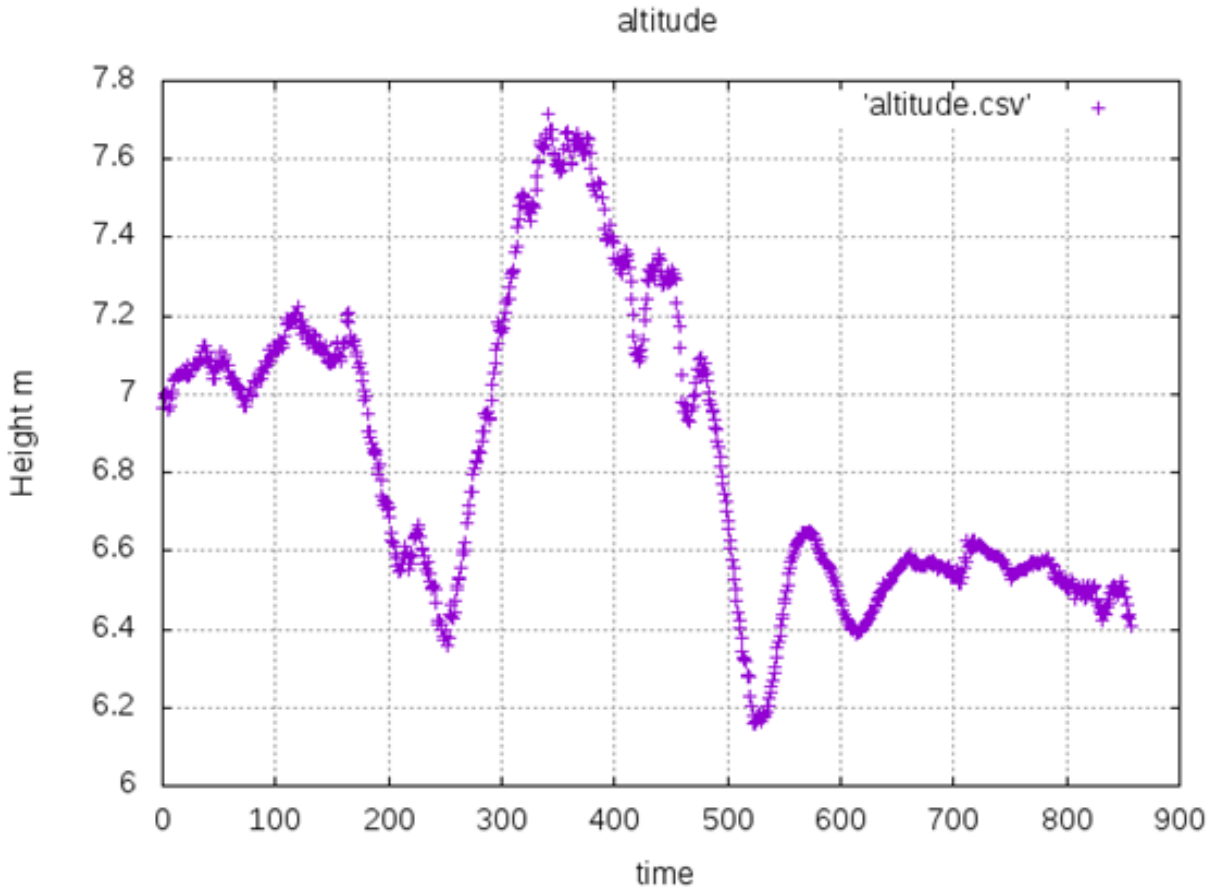
Mobile Forensics (A.R Freeflight application)

- “.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

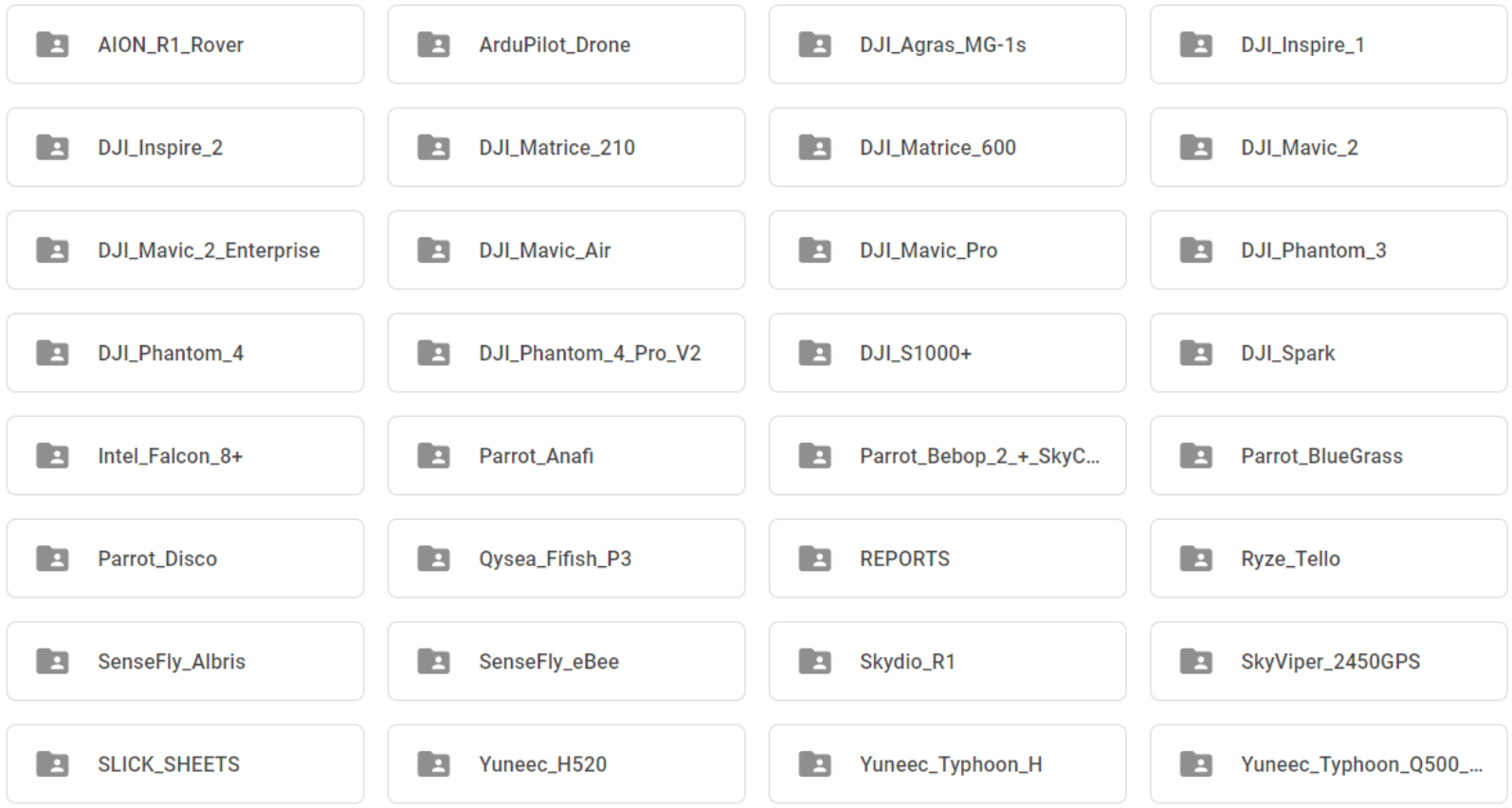
External Storage (32GB SD Card)

- 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

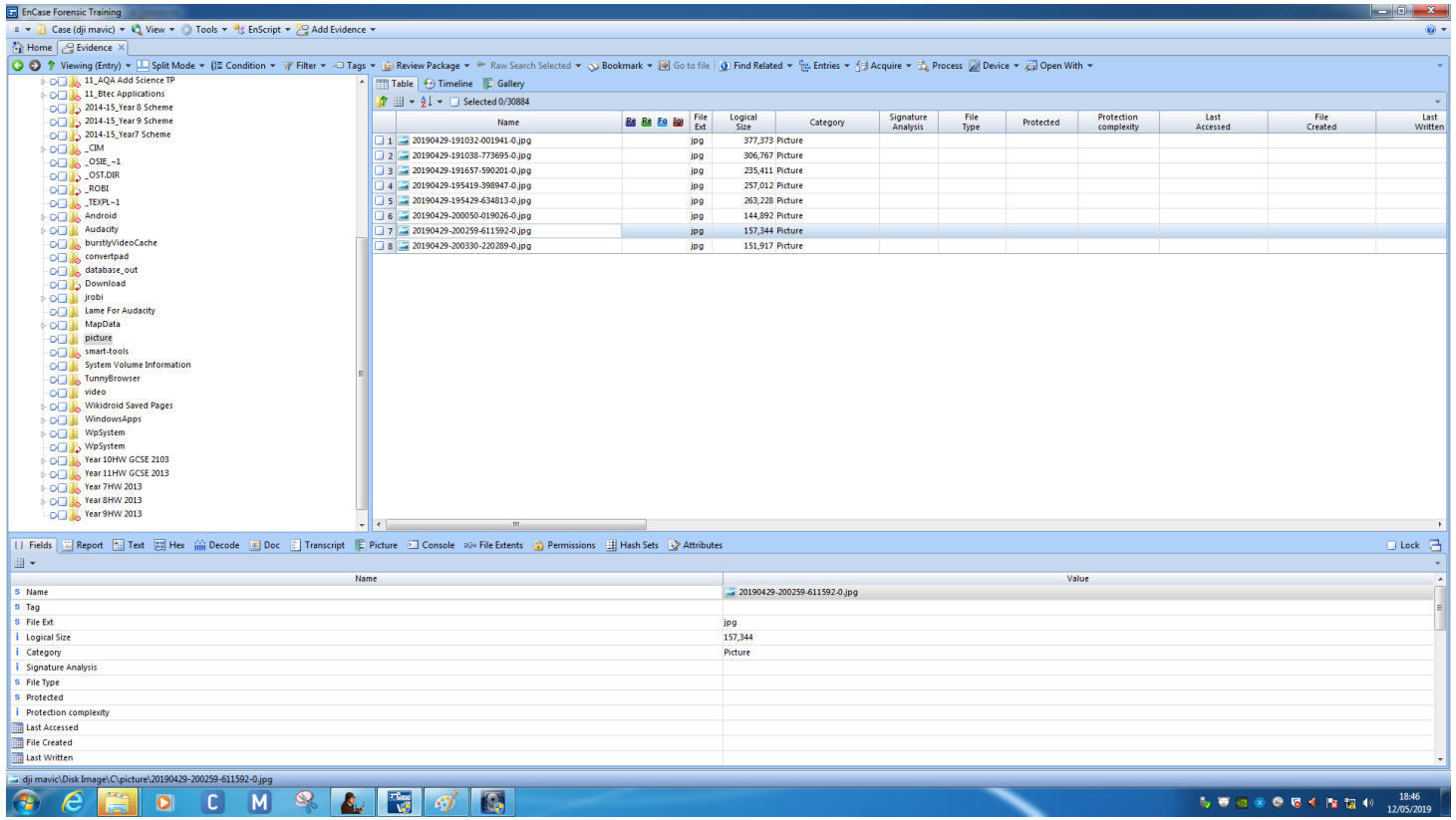


Altitude measurements for the duration of the extracted video file

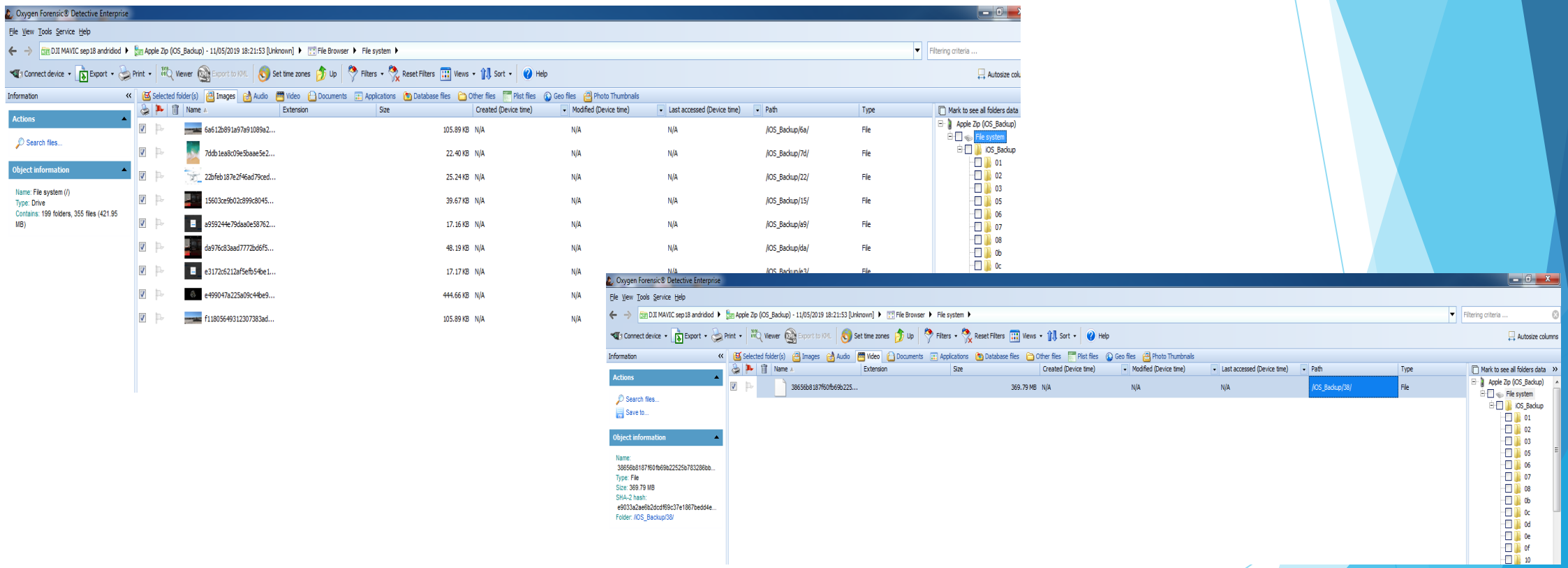
https://www.cfreds.nist.gov/drone-images.html



SD Card using FTK



Oxygen forensics



Oxygen forensics was only able to recover images and video from the apple phone backup of DJI Mavic

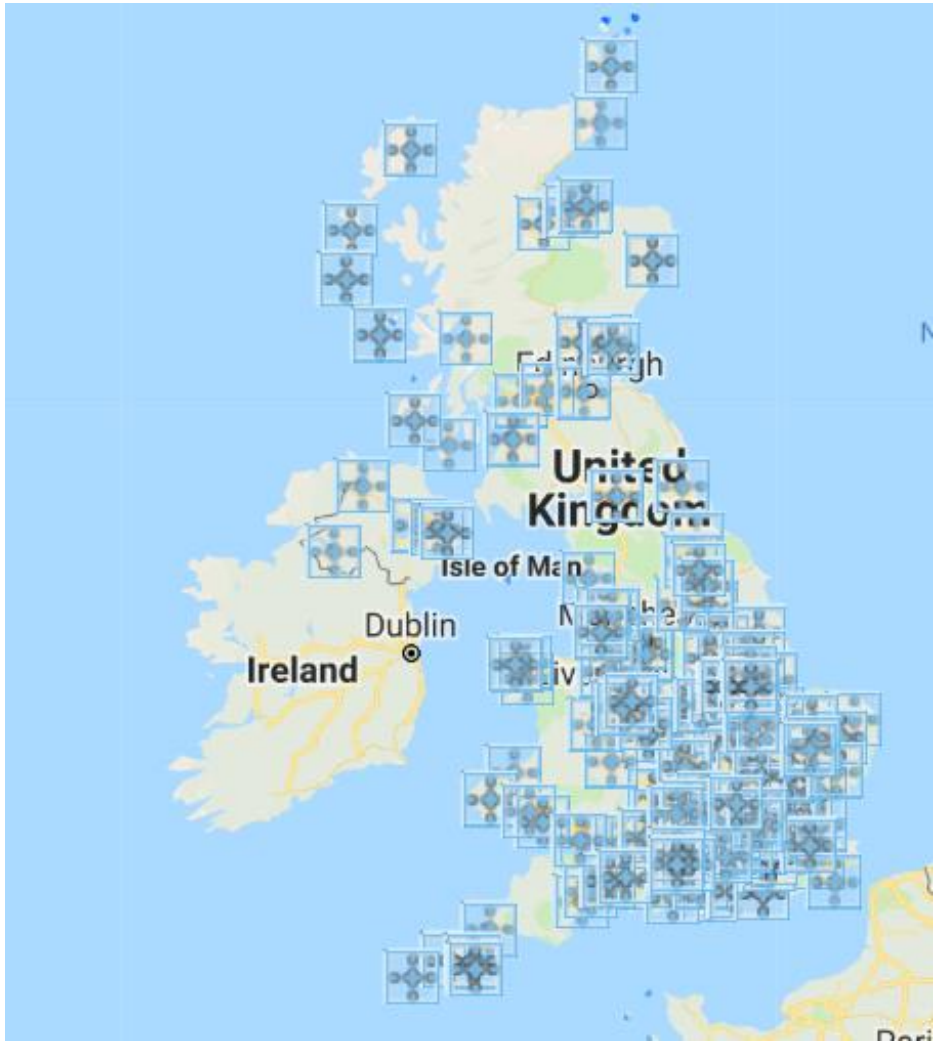
Others: Cellebrite ‘s UFED Physical analyser ; XRY Drone from MSAB

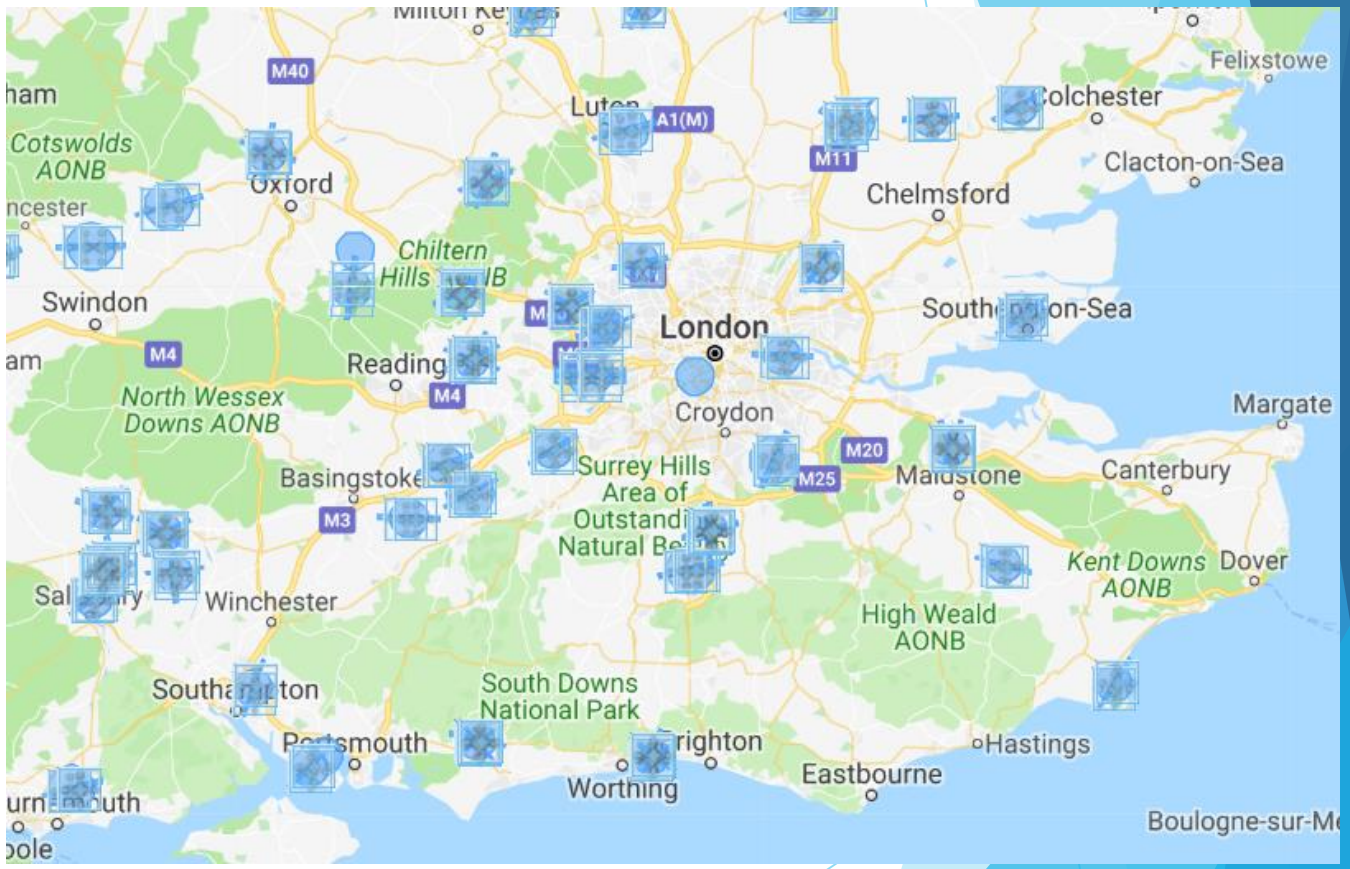
Airport restrictions

- 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/

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/
- 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:
  - Azhar, M,A.H.B; Barton, T.; and Islam, T. (2018) "*Drone Forensic Analysis Using Open Source Tools*," *Journal of Digital Forensics, Security and Law*: Vol. 13 : No. 1 , Article 6. Available at: https://commons.erau.edu/jdfsl/vol13/iss1/6
  - Barton, T. and Azhar, M.A.H.B, (2017) "*Open Source Forensics for a Multi-platform Drone System*", 9th EAI International Conference on Digital Forensics & Cyber Crime, Prague, Springer-Verlag; https://link.springer.com/chapter/10.1007/978-3-319-73697-6_6