UAV (aka drone) Forensics
Who We Are

• David Kovar
  – Commercial UAV owner/pilot
  – Ex Big 4 - Cyber security investigator, Incident response consultant

• Greg Dominguez
  – Personal UAV owner/Pilot
  – Retired Air Force Computer Crime Investigator, Ex-Big 4 Investigator, former COO of forensic hardware firm

• Cindy Murphy
  – Cellphone Forensicator extraordinaire

With thanks to Cellebrite for technical assistance
Teaching is reminding others that they know just as well as you.
- Richard Bach
Closing Opening Thoughts

The UAV is paired with controller &
The UAV is also paired with ground control station (mobile device) &
The UAV collects data that may be tagged &
Something is used to plan the mission &
The sensor data needs to be analyzed and used

Which means Unique IDs &
Forensic evidence linking devices
Connecting Evidence is Hard

“There is no SN number for the entire product, however, there is a SN number for different components. So you could use one component SN number as the unique identifier such as Flight Controller SN number.” – DJI

Seems a bit vague to you, too?
It Used to be Easy – P2 vs P3

These are just serial numbers.
No easy way to trace a hull to an individual

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>60601F</td>
<td>SZ DJI TECHNOLOGY CO., LTD</td>
</tr>
</tbody>
</table>
## UAV workflow – evidence everywhere

<table>
<thead>
<tr>
<th>Mission Planning</th>
<th>Approval</th>
<th>Execution</th>
<th>Analysis</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>‣ Criteria</td>
<td>‣ Business</td>
<td>‣ Logistics</td>
<td>‣ Data validation</td>
<td>‣ Product delivery</td>
</tr>
<tr>
<td>‣ Airframe</td>
<td>‣ Site logistics</td>
<td>‣ Flight crew</td>
<td>‣ Product generation</td>
<td>‣ Product support</td>
</tr>
<tr>
<td>‣ Payload</td>
<td>‣ Safety</td>
<td>‣ Weather</td>
<td>‣ Quality assurance</td>
<td>‣ Lessons learned</td>
</tr>
<tr>
<td>‣ Operator</td>
<td>‣ Legal</td>
<td>‣ Flight operations</td>
<td>‣ Product delivery</td>
<td>‣ Reporting</td>
</tr>
<tr>
<td>‣ Location</td>
<td>‣ Risk</td>
<td>‣ Flight operations</td>
<td>‣ Lessons learned</td>
<td>‣ Billing</td>
</tr>
<tr>
<td>‣ Time frame</td>
<td>‣ Flight operations</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
UAV data flows

GPS signals

Data uplink to cloud

Telemetry to corporate network

PIC to UAV FC via radio controller

GCS via data link to UAV FC

Payload operator via data link to UAV mission payload
DJI Phantom 3 – Example UAV

• Very common UAV
• Relatively easy to hack
• SDK available
• Demonstrates all the major components
What Physical Evidence is Available?
UAV Forensic Artifacts

**Physical**
- Drone
  - Flight controller
  - Sensor
  - Physical evidence
- Ground Station
  - Data link
  - Ground control station
  - Radio controller
- Support and Post Processing
  - Maintenance system
  - Image processing
  - Billing, R&D, et al

**Digital**
- Mobile OS
- Traditional OS
- Embedded Linux
- Variety of file systems (e.g. JFFS2)
- Media storage
- EEPROMs
- Firmware

**Other**
- Mission planning
- Maintenance logs
- Purchase records
- Social media
- Fingerprints
JTAG Analysis
Short Answer – Not Much Success

• Some chips are sealed
• Data may not persist across reboots
• Further analysis required
The Internals – MCU and GPS
But, there is an ID ....
Log Analysis
UAV Exam – Data Logging (Black Box)

• Many flight controllers, PixHawk for example, have data logging capabilities included

• Others, such as the DJI Naza, require an off board data logger

• Most ground control station applications have data logging capabilities
Phantom 3 Logs

• The Phantom 3 series (Professional, Advanced and Standard) create very similar logs
  – UAV Flight Data Recorder creates FLY????.DAT files
  – The GCS or DJI GO.app creates DJIFLightRecord_date/time.TXT files
  – The ??? are a 3 digit sequence number
  – The logs will have a Date Time stamp
Phantom 3 Log Collection

• **FLY???.DAT**
  - Are stored on a 4GB microSD card on the bottom side of the Main Board inside the UAV
  - The UAV will push oldest .DAT out for newest
  - To remove the card the UAV must opened
    • Not a simple task, but doable
    • Video link:  
      [https://www.youtube.com/watch?v=MNQUQ8p9IGE](https://www.youtube.com/watch?v=MNQUQ8p9IGE)
Connecting Logs to the Airframe

• The MC ID will look like: “MC ID :03Z0303948”
  – It will be about 5 lines from the bottom of the file

• Also present in:
  – DJI GO.app - DJIFlightRecord_2016-03-27_[10-06-08].txt
  – On the mobile device in various applications
  – Chip on main board
  – Data stream?
FLY???.DAT - DatCon

• DatCon (web app) creates the following files
  – FLY???.csv (huge very detailed spreadsheet)
  – FLY???.kml (if you ask it to) used to plug into Google Earth to see the flight track
  – FLY???.log.txt
  – FLY???.config.txt (Configuration log – contains MC ID)
FLY???.DAT - FLY???.csv

- Seriously detailed Data
  - Over 100 columns of data
- GPS coordinates will give interesting location data
- Primary purpose is to log all flight data like a real “BLACK BOX”
  - Battery voltage, Battery load
  - Motor load, motor speed, etc
- Data may show a crash was a system failure, not an intentional act.
FLY???.DAT - Event Log

• Shows what amounts to a Boot sequence
• Shows Board:”wm320v2”
  – wm320 is one of the Professional model numbers
• Shows the Battery barcode: 6171153003445
  – It is on the battery, the serial number is not on the battery
  – Also, has First Home Point Lat & Long
FLY???.DAT - Configuration Log

• More boot-initialization information
• The important piece in this text file is the MC ID: or UAV Serial Number
  – This is not the serial number on the outside of the UAV or on the Retail Box
  – It ties the physical airframe to the logs to the mobile device
The Answer is Often in the Data
Sensor and Sensor Data

• The type of sensor will tell you a lot about the purpose of the flight
  • LIDAR
  • Optical
  • NVIR
  • Thermal
  • WiFi

• The sensor data will tell you a lot about where it has been, particularly since GPS data is critical for most types of missions
Sensors – Optical

Most common sensor out there
  – Consumer - GoPro, DJI, Canon, Sony
  – Pro-sumer and professional

Artifacts
  – The image
  – The EXIF data

Location
  – Right there on the UAV – pull the SD card
Sensors – EXIF Data

The purpose of a camera is to take a picture, and EXIF data tells a story about the camera and where it was taking pictures.

- Image Description: DCIM\100MEDIA\DJI_0030.JPG
- Make: DJI
- Camera Model Name: FC300S
- Date/Time Original: 2016:03:27 10:15:57
- Create Date: 2016:03:27 10:15:57
- GPS Version ID: 3.2.0.0
- GPS Latitude Ref: North
- GPS Longitude Ref: West
- GPS Altitude Ref: Above Sea Level
- Aperture: 2.8
- GPS Altitude: 74.6 m Above Sea Level
- GPS Latitude: 40 deg 32' 15.84" N
- GPS Longitude: 89 deg 30' 50.63" W
- GPS Position: 40 deg 32' 15.84" N, 89 deg 30' 50.63" W

DJI Phantoms did not record altitude in the EXIF data unfortunately.
Sensors – EXIF Data
Sensor Data - Cloud

• **Consumer**
  – YouTube
  – Facebook
  – Etc

• **Commercial**
  – Data Mapper
  – Airware
  – Vendor specific

**Question:** Where are the credentials for uploading the imagery data to the cloud?
Ground Control Station/Mobile Device
Ground Control Station

- The vast majority of consumer UAVs and many commercial UAVs are controlled by a mobile device (the Ground Control Station) paired with a radio controller.
- The GCS is used for mission planning and flight operations:
  - Contains both plans and flight telemetry data
  - Often connects to, and logs to, cloud services
  - Vendor applications and community developed
- Looking for:
  - Default settings
  - Launch points, dates
  - Owner name, account
DJI Flight Record

- Recorded by the GCS app (DJI Go.app)
- Data is sent from UAV
- Subset of data in FLY????.DAT
- Can contain thumbnail images and video
- Also contains the MC ID number
DJI Flight Record

• Photos can be carved manually with Winhex
  Header: 0xFFD8FFE000104A464946
  EOF: 0xFFD9

• All of the JPG files are together at the bottom of the file

• Still dissecting the data fields
DJI Flight Record

• There is an online parser:
  http://healthydrones.com

• Remember this is online and you are sending them the file

• Will allow you to download the .csv and kml

• Has other information also
• Healthy Drones view
• Shows the flight path
• Shows the plane name
• Shows other data in the other categories
• The address may even be in the Details section
GCS – Application Data

Drone Deploy:
- ajs_user_id
- %22dkovar%40kovarllc.com%22

Pix4D:
- 2016-03-27 10:34:03 [V] [WaypointCustomMissionDJI3::87] create wp at (40.538689,-89.513918) altitude: 50.000000
- displayBtnLogout(YES,username: dkovar@gmail.com)
- 2016-03-27 11:25:24 [D] [AppDelegate::38]

DJI Pilot:
- kUserDefaultKeyAircraftLocation – 4x.xxx448,-8x.xxx675,-1577 (My house)
- com.facebook.sdk:serverConfiguration1383125992006153-<62706c69 73743030 >
UAS Exam – Remember that MC ID?

./com.dji.pilot/Documents/.device/history & ./com.dji.pilot/Library/Preferences/com.dji.pilot.plist

- version="1.0">string>03Z0303948&amp;02.04.10.07</string></plist>

com.facebook.sdk:serverConfiguration1383125992006153 - <62706c6973743030>

statistics.db

- {user=Anonymous&amp;apptype=0&amp;appversion=2522&amp;devicetype=2&amp;deviceversion=01.07.00.00&amp;devicesn=7130333511&amp;producttype=3&amp;createtime=1459090198.971318&amp;guid=F7F0A647-B460-41AD-B876-AD971E6079C1
- {user=Anonymous&amp;apptype=0&amp;appversion=2522&amp;devicetype=1&amp;deviceversion=02.04.10.07&amp;devicesn=03Z0303948&amp;producttype=3&amp;createtime=1459090197.770736&amp;guid=A8B53105-8B50-4F36-AAC9-3C5C09D5023D
- {user=Anonymous&amp;apptype=0&amp;appversion=2522&amp;devicetype=0&amp;deviceversion=01.22.40.95&amp;devicesn=04CLA51862&amp;producttype=3&amp;createtime=1459090196.597396&amp;guid=9C244F41-6F0A-4767-9930-78C74CED66FÄ;
- {user=Anonymous&amp;apptype=0&amp;appversion=2522&amp;devicetype=2&amp;deviceversion=01.07.15.01&amp;devicesn=5443003511&amp;producttype=3&amp;createtime=1459095943.455033&amp;guid=CDB1637E-E9D7-458E-B859-0FD3DC007ACC

Devicetype=1 – Airframe  Devicetype=2 – Battery  Devicetype=3 – Camera

Airframe tied to camera tied to multiple batteries tied to a mobile device tied to log files tied to images.
Analysis of Other UAVs
UAVs with PixHawk Flight Controller

The following was created in under two minutes using Mission Planner
UAVs with Pixhawk Flight Controller

And this is what a crash looks like ....
### UAVs with PixHawk Flight Controller

And all flight parameters are easily collected

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS_BATT_MAH</td>
<td>0</td>
</tr>
<tr>
<td>MIS_RESTART</td>
<td>0</td>
</tr>
<tr>
<td>AFS_WP_COMM</td>
<td>0</td>
</tr>
<tr>
<td>INS_ACOFFS_Z</td>
<td>-0.3554053</td>
</tr>
<tr>
<td>AFS_ENABLE</td>
<td>0</td>
</tr>
<tr>
<td>RLL25RVS_I</td>
<td>0.1</td>
</tr>
<tr>
<td>PITCH2SRV_TCONST</td>
<td>0.5</td>
</tr>
<tr>
<td>EKF_WIND_PNOISE</td>
<td>0.1</td>
</tr>
<tr>
<td>RNGFND_OFFSET</td>
<td>0</td>
</tr>
<tr>
<td>BATT2_MONITOR</td>
<td>0</td>
</tr>
<tr>
<td>FBWB_ELEV_REV</td>
<td>0</td>
</tr>
<tr>
<td>TERRAIN_ENABLE</td>
<td>1</td>
</tr>
<tr>
<td>ALT_HOLD_RTL</td>
<td>10000</td>
</tr>
<tr>
<td>ELEVON_OUTPUT</td>
<td>0</td>
</tr>
<tr>
<td>ARMING_REQUIRE</td>
<td>0</td>
</tr>
<tr>
<td>RLL25RVS_D</td>
<td>0.1</td>
</tr>
<tr>
<td>RMAP_PITCH</td>
<td>2</td>
</tr>
<tr>
<td>EKF_GYRO_PNOISE</td>
<td>0.015</td>
</tr>
<tr>
<td>SR0_EXTRA3</td>
<td>2</td>
</tr>
<tr>
<td>AFS_TERM_PIN</td>
<td>-1</td>
</tr>
<tr>
<td>RELAY_DEFAULT</td>
<td>0</td>
</tr>
<tr>
<td>SR0_POSITION</td>
<td>3</td>
</tr>
<tr>
<td>AUTO_FBW_STEER</td>
<td>0</td>
</tr>
<tr>
<td>ALT_OFFSET</td>
<td>0</td>
</tr>
<tr>
<td>TEC5_LAND_ASPD</td>
<td>-1</td>
</tr>
<tr>
<td>FORMAT_VERSION</td>
<td>13</td>
</tr>
<tr>
<td>BATT2_VOLT_PIN</td>
<td>2</td>
</tr>
<tr>
<td>AHRS_GPS_MINSATS</td>
<td>6</td>
</tr>
<tr>
<td>RALLY_TOTAL</td>
<td>0</td>
</tr>
<tr>
<td>RC1_02</td>
<td>30</td>
</tr>
</tbody>
</table>
Closing Thoughts
Challenges & Solutions

• Data and command & control moving from WiFi to Bluetooth to dedicated radio to LTE & 4G
  • Harder to hack, easier to triangulate and identify with existing tools

• Many vendors, lots of variety, embedded systems

• Focus on ground control stations and post processing systems, analyze the sensor data. They tell 80% of the story
Closing Thoughts - Forensics

- We needed to analyze the following to cover the entire system:
  - Three different versions of Linux
  - IOS or Android
  - OS X or Windows
  - 6+ file systems
  - ser2net
  - Wifi or Bluetooth or 915Mhz data link
  - EXIF
  - GPS
  - “Social media”
  - SDK

No single UAV analysis tool
Closing Thoughts

• Cybersecurity:

• The proper term for drones is sUAS – small unmanned aerial system. Take a system approach to security and investigations, do not treat the vehicle as a discreet or standalone element.

• Law & Policy:

• UAVVehicle. Apply law and policy to the risk/threat posed by the sensors and services rather than by the delivery mechanism

• Federal agencies using UAVs should consider Federal guidance on data protection and retention - http://www.justice.gov/file/441266/download