UAV (aka drone) Forensics

June 5-8, 2016 Myrtle Beach, SC USA

Techno Security & Forensics Investigations Conference

Mobile Forensics World

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

Why is the Relevant?

Market Growth and Jobs

- FAA - Drone sales are expected to grow from 2.5 million this year to 7 million in 2020
- AUVSI's *The Economic Impact of Unmanned Aircraft Systems Integration in the United States* report shows the economic benefit of UAS integration. AUVSI's findings show that in the first three years of integration more than 70,000 jobs will be created in the United States with an economic impact of more than $13.6 billion. This benefit will grow through 2025 when we foresee more than 100,000 jobs created and economic impact of $82 billion.
- According to OpenSecrets.org, which tracks the influence of Washington lobbyists, spending by groups pushing for drone legalization has exploded from $35 million in 2011 to $184 million last year
- 20,000 DJI drones sold per month

Illegal and inappropriate activity

- Drug delivery over US/Mexico border
- Drug and weapon delivery to prison
- Multiple invasions of privacy
- Flight above crowds and in controlled airspace
- Flight into operators and bystanders

If You Are in Law Enforcement

- “There is evidence of a considerable increase in the unauthorized use of small, inexpensive Unmanned Aircraft Systems (UAS) by individuals and organizations, including companies. The FAA retains the responsibility for enforcing Federal Aviation Regulations, including those applicable to the use of UAS. The agency recognizes though that State and local Law Enforcement Agencies (LEA) are often in the best position to deter, detect, immediately investigate, and, as appropriate, pursue enforcement actions to stop unauthorized or unsafe UAS operations.”

- https://www.faa.gov/uas/regulations_policies/media/FAA_UAS-PO_LEA_Guidance.pdf

Anti-drone Solutions

- RF fingerprinting
- Jamming
- Geo-fencing and no fly zones
- Tangle-drone – Drops net over drone
- Shotguns
- Debris and game jerseys
- Lasers

Terminology

- UAS – Unmanned Aerial System – Emphasis on system
- UAV – Unmanned Aerial Vehicle – The aircraft portion of the system
- GCS – Ground Control Station – The flight control portion of the system. May include manual and automatic control features
- Data link – radio system to transmit data to and from the UAV. Often used for telemetry, sensor data, and FPV operation
- Drone – Common term for any UAV but most often used to describe quads and other multirotor UAVs
- FPV – First Person View – technology that enables the operator to fly the UAV from the perspective of the UAV

Drone Forensics – High Altitude View

June 5-8, 2016 Myrtle Beach, SC USA

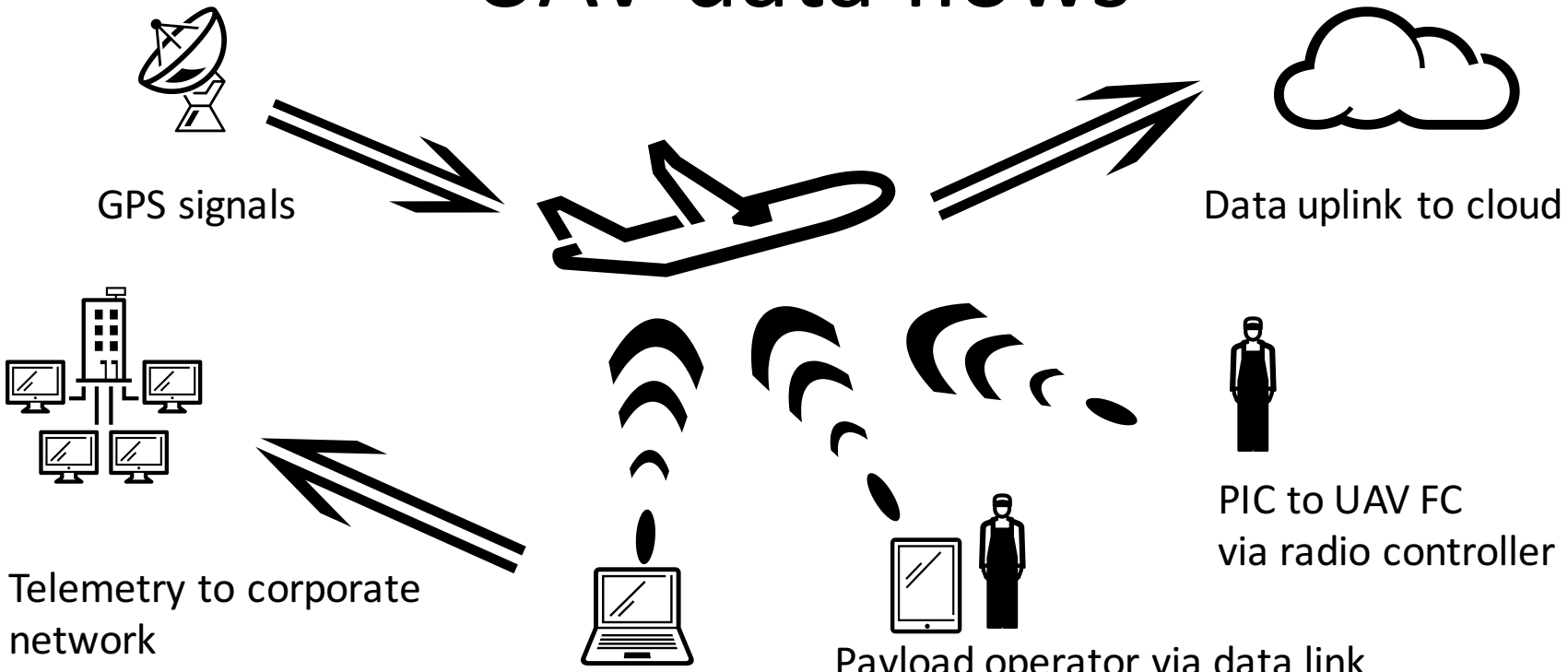
Techno Security & Forensics Investigations Conference

Mobile Forensics World

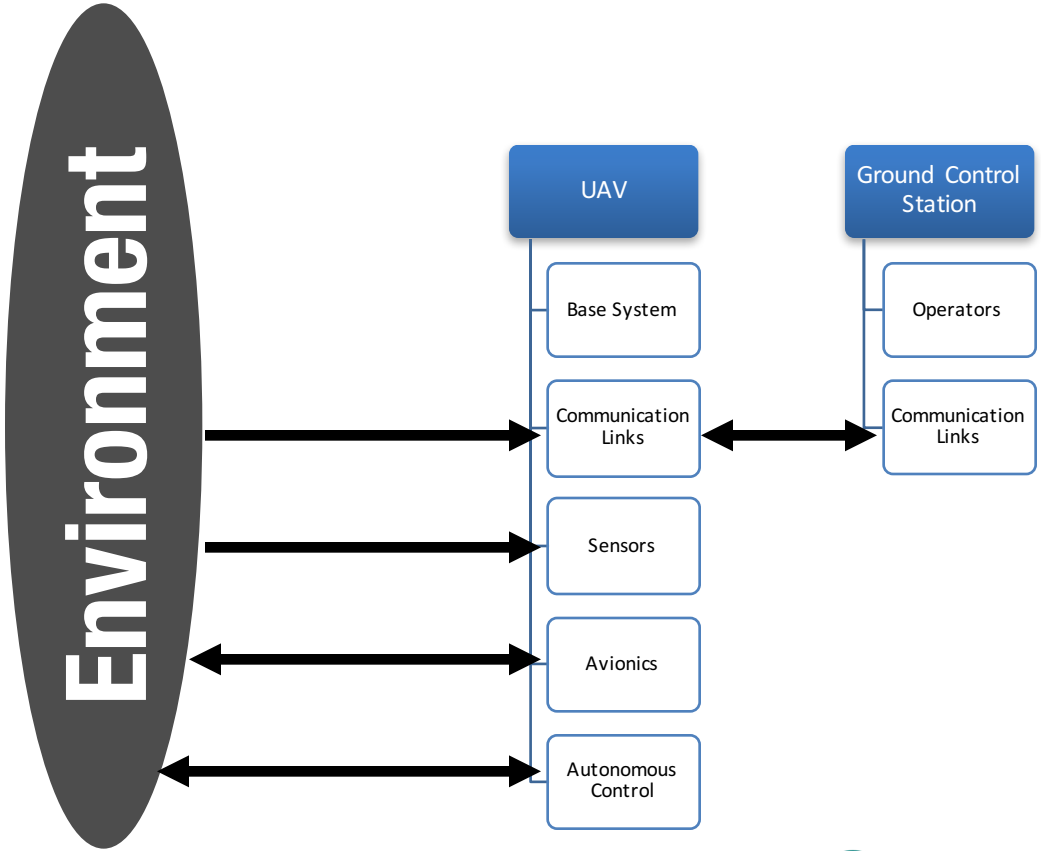
UAV workflow

Mission Planning	Approval	Execution	Analysis	Delivery
Criteria	Business	Logistics	Data validation	Product delivery
Airframe	Site logistics	Flight crew	Product generation	Product support
Payload	Safety	Weather	Quality assurance	Lessons learned
Operator	Legal	Flight operations		Reporting
Location	Risk			Billing
Time frame	Flight operations			

UAV data flows



Operator, UAV, Environment Flows



DJI Phantom 3 – Example UAV

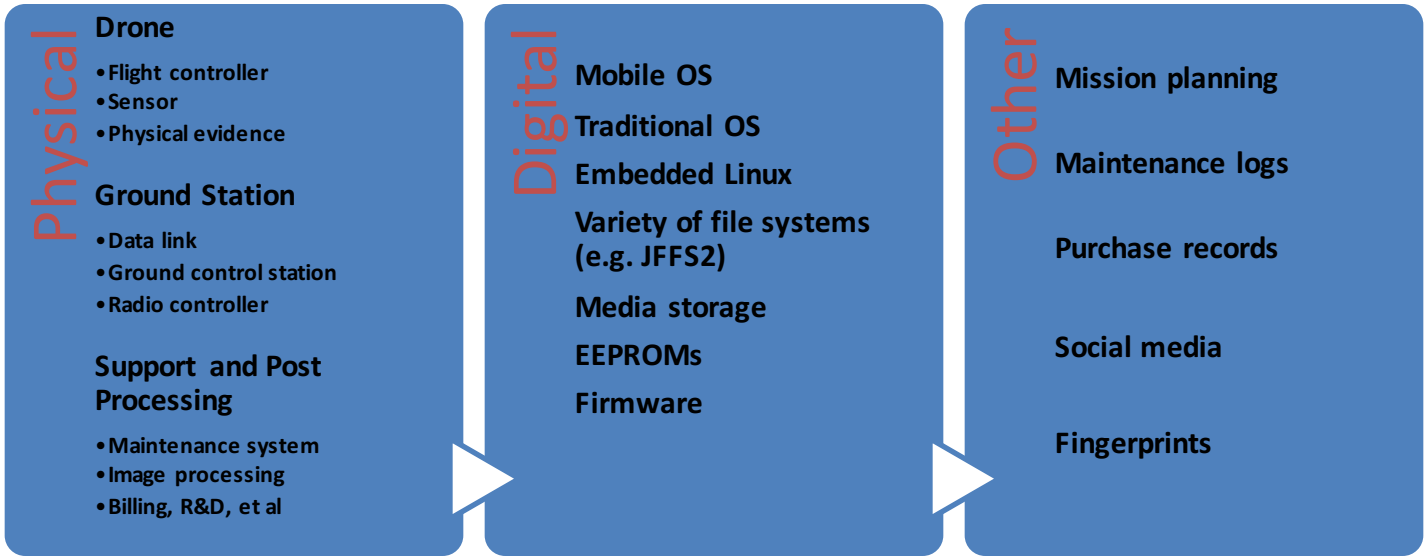
- **Very common UAV**
- **Relatively easy to hack**
- **SDK available**
- **Demonstrates all the major components**

Connecting Evidence is Hard

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

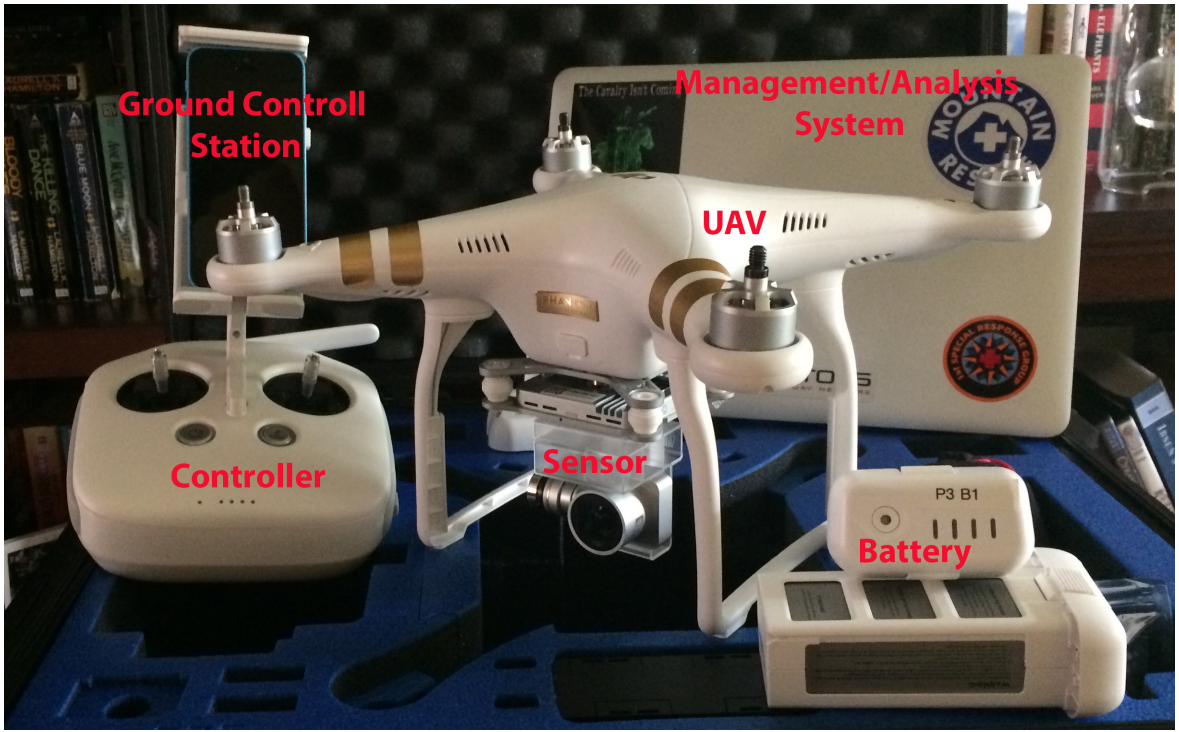
- DJI

UAV Forensic Artifacts



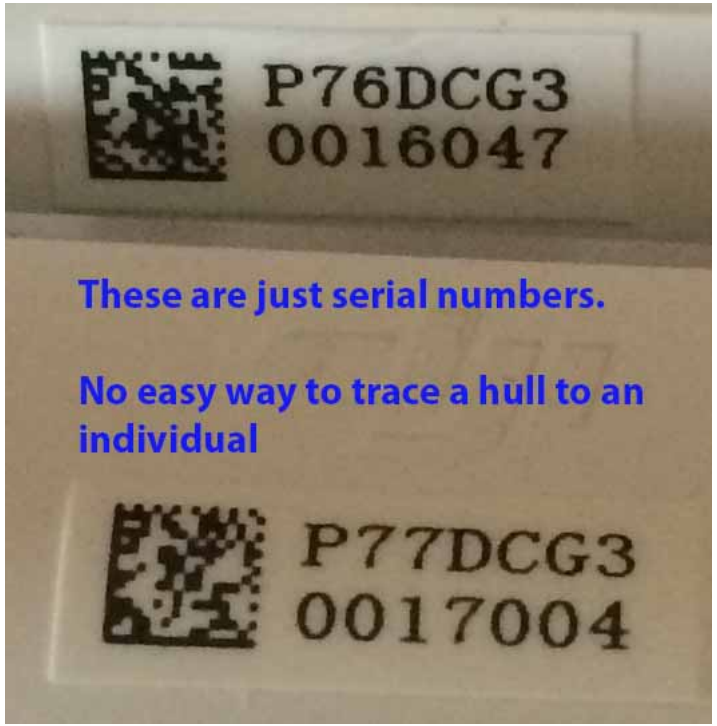
Physical Artifacts

What Physical Evidence is Available?



Phantom 2 vs Phantom 3

Prefix	Vendor
60601F	SZ DJI TECHNOLOGY CO.,LTD



Systems

UAV CPUs & “operating systems”

The flight controller is the core system in a UAS and amounts to the aircraft’s CPU & operating system.

Open Source	Commercial
➢ Openpilot	➢ Parrot AR Drone FC
➢ Ardupilot (APM, Pixihawk)	➢ Naza (DJI)
➢ Multiwii	➢ Wookong (DJI)
➢ KKmultipcopter	➢ Dualsky (FC450, etc)

- Airware is trying to be the Microsoft/IBM of the UAV world, selling hardware and software that they hope is the defacto standard for flight controllers.

- Linux is the predominant OS for onboard UAV systems

UAV Exam – SDKs and Live UAV

- Most of the flight data is in RAM and most of the flight controller software is running off of flash media. Very little useful data persists after power is removed other than sensor data on the removable media.
- Similar to many other “normal” systems, APIs and SDKs exist for UAVs.
- Most commercial UAV applications will not extract all of the data an analyst needs.
- Be prepared to develop your own investigative tools using SDKs.

UAV Exam – SDKs and Live UAV

- Battery:
  {designedVolume=5200|fullChargeVolume=5200|currentElectricity=4141|currentVoltage=11876|currentCurrent=-961|remainLifePercent=100|remainPowerPercent=79|batteryTemperature=20|dischargeCount=2|}

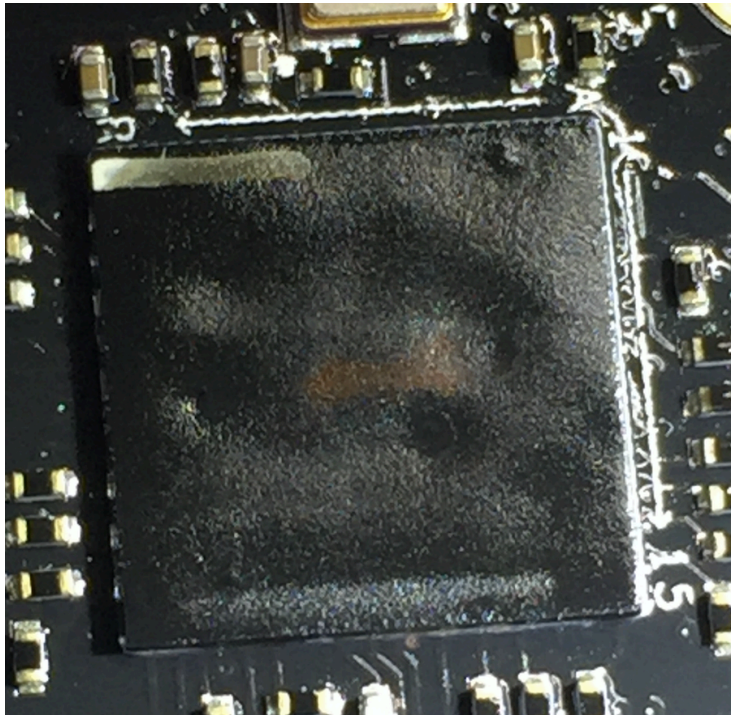
- MC:
  {satelliteCount=6.0|homeLocationLatitude=40.4314293|homeLocationLongitude=-89.31180890000002|phantomLocationLatitude=40.4314619|phantomLocationLongitude=-89.31181570000001|velocityX=0.0|velocityY=0.0|velocityZ=-1.0|speed=0.1|altitude=-8.31500244140625|pitch=0.0|roll=-1.0|yaw=-120.0|remainPower=11878.0|remainFlyTime=0.0|powerLevel=2.0|isFlying=false|noFlyStatus=0.0|noFlyZoneCenterLatitude=0.0|noFlyZoneCenterLongitude=0.0|noFlyZoneRadius=0.0|}

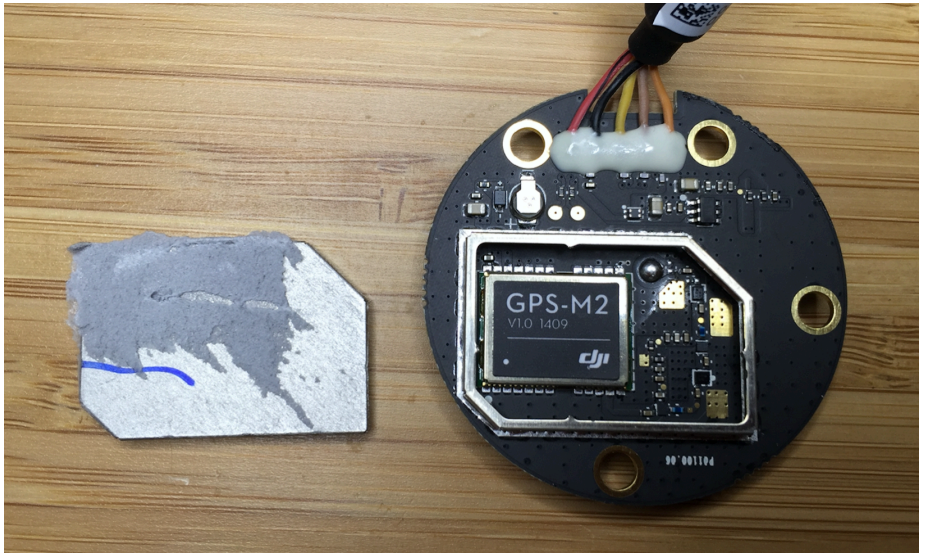
JTAG Analysis

Short Answer – Not Much Success

- Some chips are sealed
- Data may not persist across reboots
- Further analysis required

The Internals – MCU and GPS





Log Analysis

UAV Exam – Data Logging (Black Box)

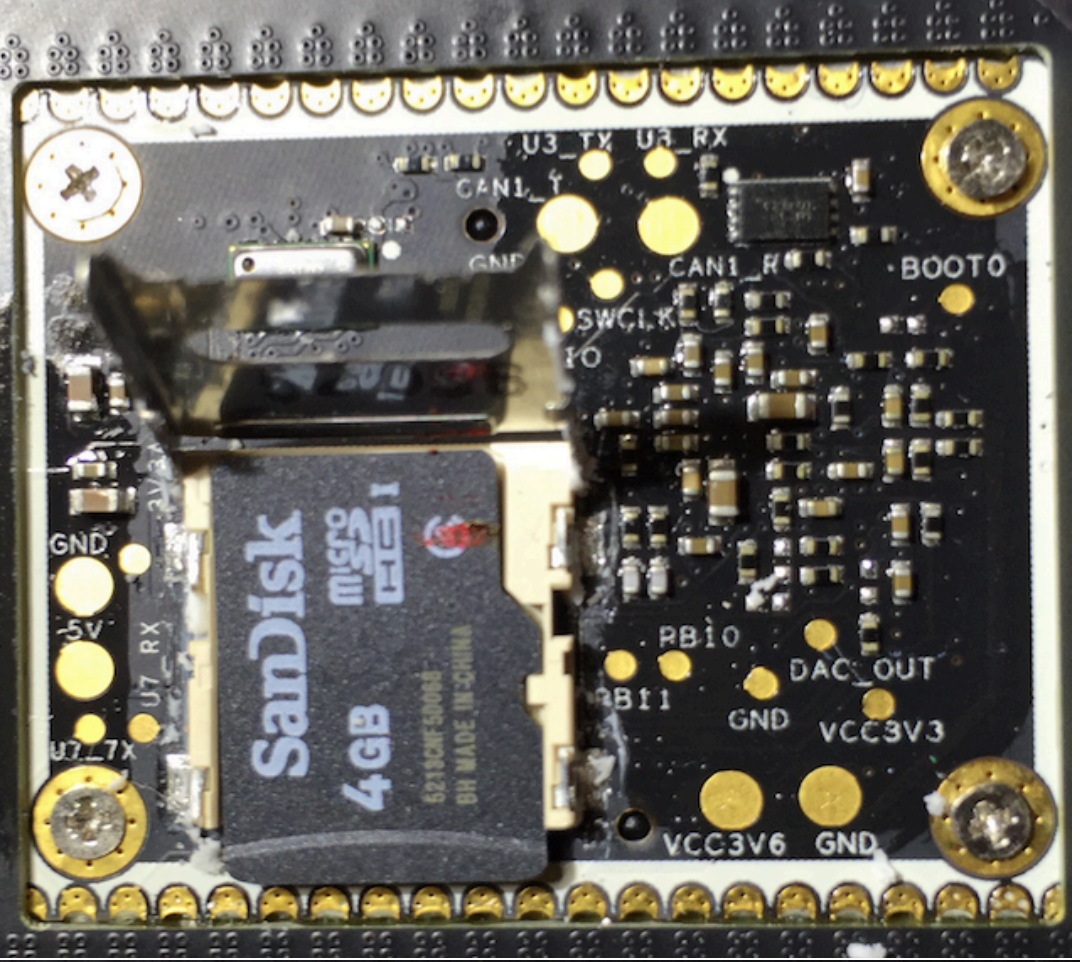
- Many flight controllers, PixHawk for example, have data logging capabilities included
- Others, such as the DJI Naza, require an off board data logger
- Some ground control station applications have data logging capabilities

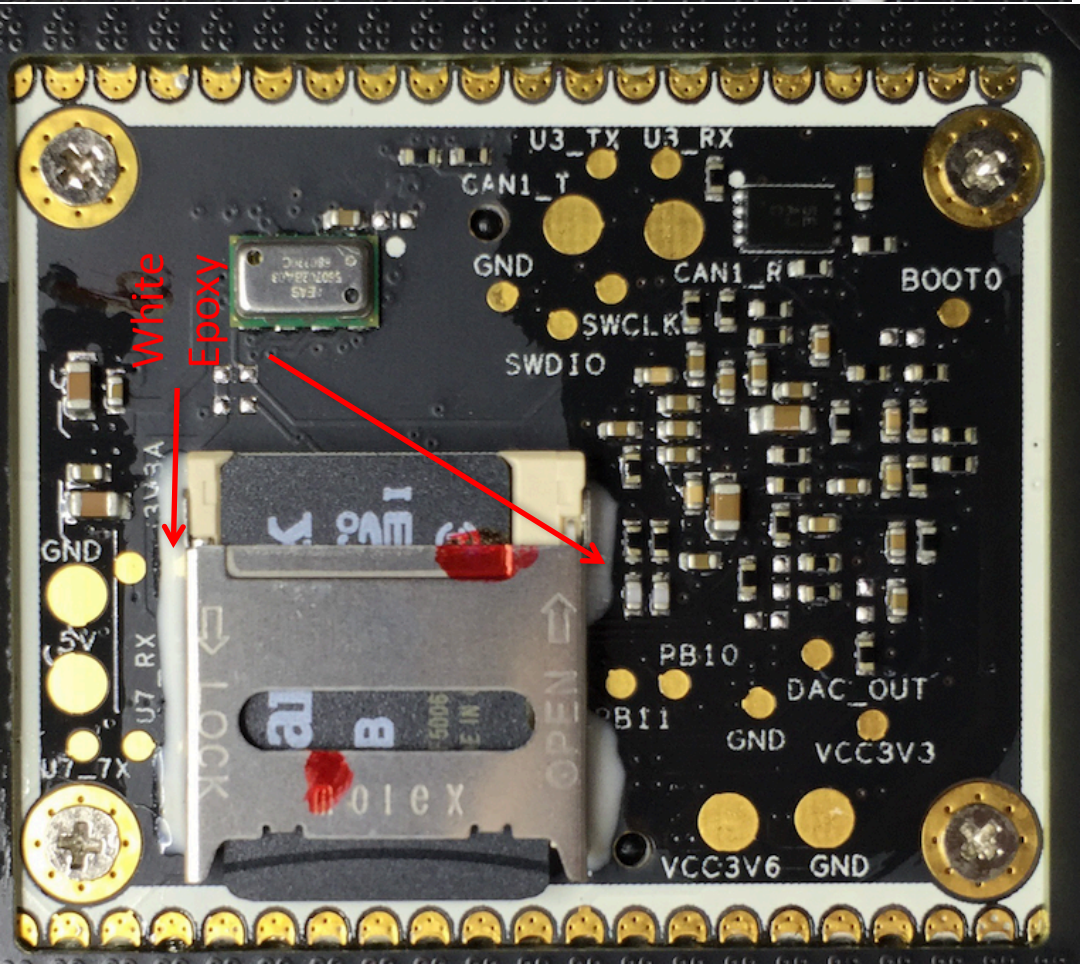
Phantom 3 Logs

- 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 up
    - Not a simple task, but doable
    - Video link: https://www.youtube.com/watch?v=MNQUQ8p9IGE

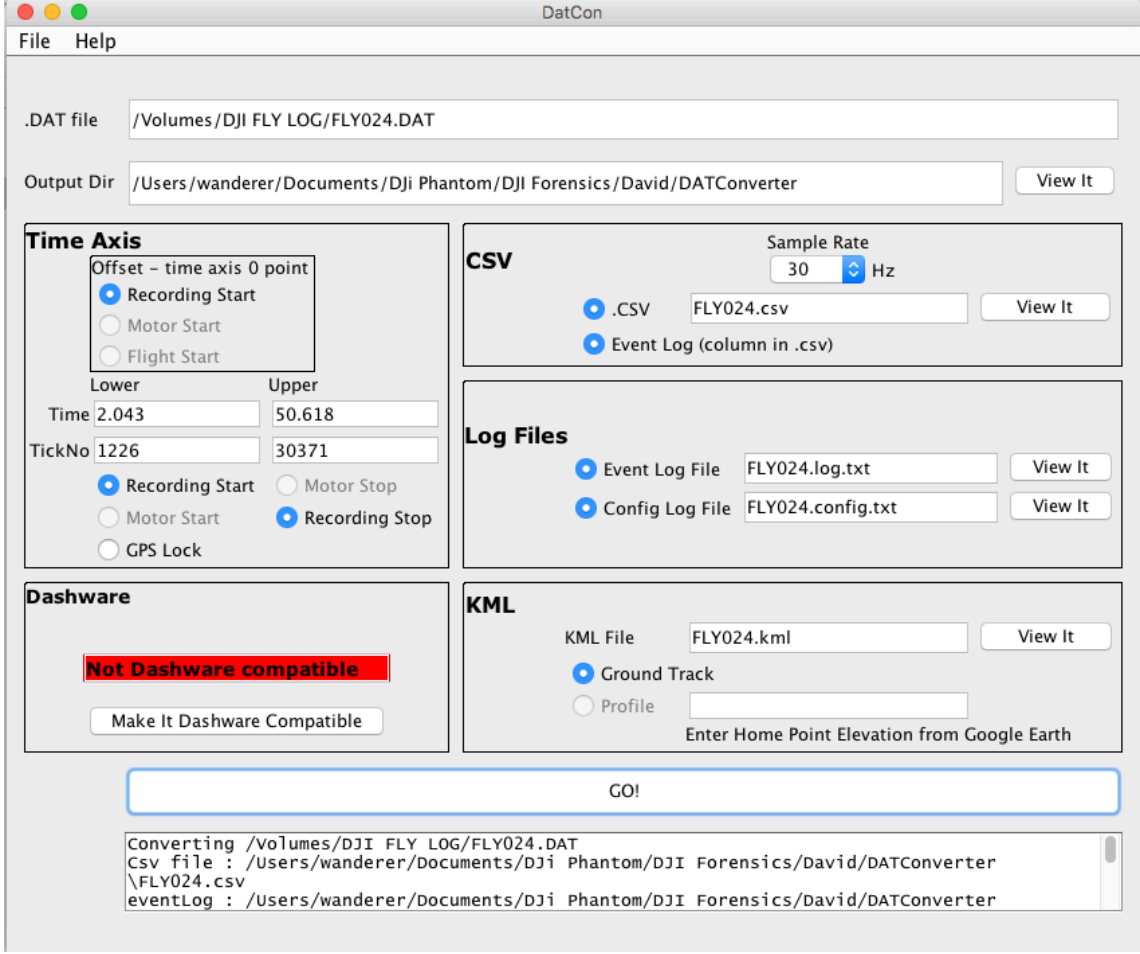

U3_TX
U3_RX
CAN1_T
GND
CAN1_R
BOOT0
SWCLK
IO
SanDisk
4GB
GND
5V
U7_RX
U7_TX
PB10
PB11
DAC_OUT
GND
VCC3V3
VCC3V6
GND


White
Epoxy
U3_TX
U3_RX
CAN1_T
GND
CAN1_R
BOOT0
SWCLK
SWDIO
GND
5V
U7_RX
U7_TX
PB10
PB11
DAC_OUT
GND
VCC3V3
VCC3V6
GND
Lock
OPEN
Molex

FLY???.DAT

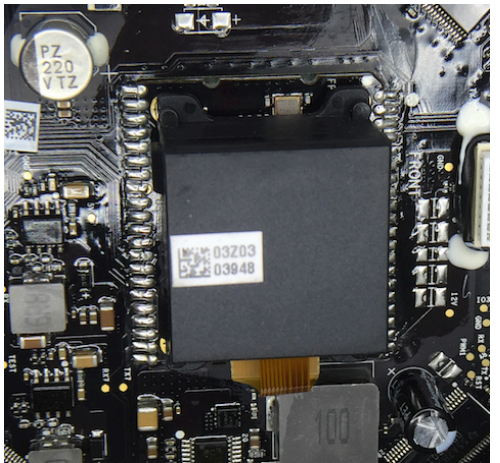
- Remove the micro SD Card and image it
- Extract the .DAT file with the most recent date
- Use DatCon.exe a FREE application from Rowland Johnson https://datfile.net
- DatCon will extract a mountain of information
  - Mostly Flight Data (GPS, battery, motor, altitude, etc)
  - DatCon is designed to assist in crash cause determination

- Runs on PC, Mac, Linux
- DatCon converts the Flight Data Record from the UAV
- You have a bit of latitude in what it gives you
- You may want to run it a few times with different settings
- For Instance – selecting “Recording Start” gives you data starting before GPS Lock that includes the UAV serial number or “MC ID:”



DatCon

- The MC ID will look like: 12482 :
  MC ID :03Z0303948
  - It will be about 5 lines from the bottom of the file
  - This number is also on a label on the Main Controller on the main board
  - FYI – The number is also in the DJIFlightRecord_2016-03-27_[10-06-08].txt
    - Created by the DJI GO.app
  - And it is on the mobile device in various applications



DatCon

- DatCon 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???.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.

205	5900	9.833	0	0	0	7	205.0844	0		0	0.00370012
206	5921	9.868	0	0	0	7	204.82642	0		0	0.00369795
207	5942	9.903	0	0	0	7	204.9422	0		0	0.00418394
208	5963	9.938	0	0	0	7	205.78519	0		0	0.00306508
209	5984	9.973	0	0	0	7	204.53592	0		0	0.00353689
210	6005	10.008	0	0	0	7	205.88269	0		0	0.0035738
211	6026	10.043	0	0	0	7	205.88269	0		0	0.0035738
212	6047	10.078	0	-89.311684	40.4314889	7	204.73094	204.73094		0	0.00481765
213	6068	10.113	0	-89.311684	40.4314889	7	204.83455	204.96506		0	0.00347734
214	6089	10.148	0	-89.311684	40.4314889	7	205.32309	204.9676		0	0.00364866
215	6110	10.183	0	-89.311684	40.4314889	7	205.30276	204.96878		0	0.00454843
216	6131	10.218	0	-89.311684	40.4314889	7	204.79594	204.97665		0	0.00495827
217	6152	10.253	0	-89.311684	40.4314889	7	205.01433	204.9794		0	0.00442651
218	6172	10.287	0	-89.311682	40.431489	7	204.99197	204.98044	0.26354837	0	0.00417114
219	6194	10.323	0	-89.311682	40.431489	7	205.59831	204.98344	0.26719138	0	0.00399192
220	6215	10.358	0	-89.311682	40.431489	7	205.22356	204.98784	0.2704626	0	0.00451291
221	6236	10.393	0	-89.311682	40.4314892	7	204.58975	204.99129	0.27081573	0	0.00460048
222	6257	10.428	0	-89.311682	40.4314892	7	205.058	204.99225	0.27109057	0	0.00432047
223	6278	10.463	0	-89.311681	40.4314891	7	205.51707	204.99295	0.27339354	0	0.00467972
224	6299	10.498	0	-89.311681	40.4314891	7	205.13417	204.99583	0.27404606	0	0.00415297
225	6320	10.533	0	-89.311681	40.4314891	7	204.26878	204.99767	0.2747182	0	0.00359667
226	6341	10.568	0	-89.311681	40.4314891	7	204.87111	205.00235	0.2806532	0	0.0045848

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

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

DJI Flight Record

- Recorded by the GCS app (DJI Go.app)
- Data is sent from UAV
- Has Flight data similar to the Flight Record
  - Just not as much
- Can contain images and video
- Also contains the MC ID number

DJI Flight Record

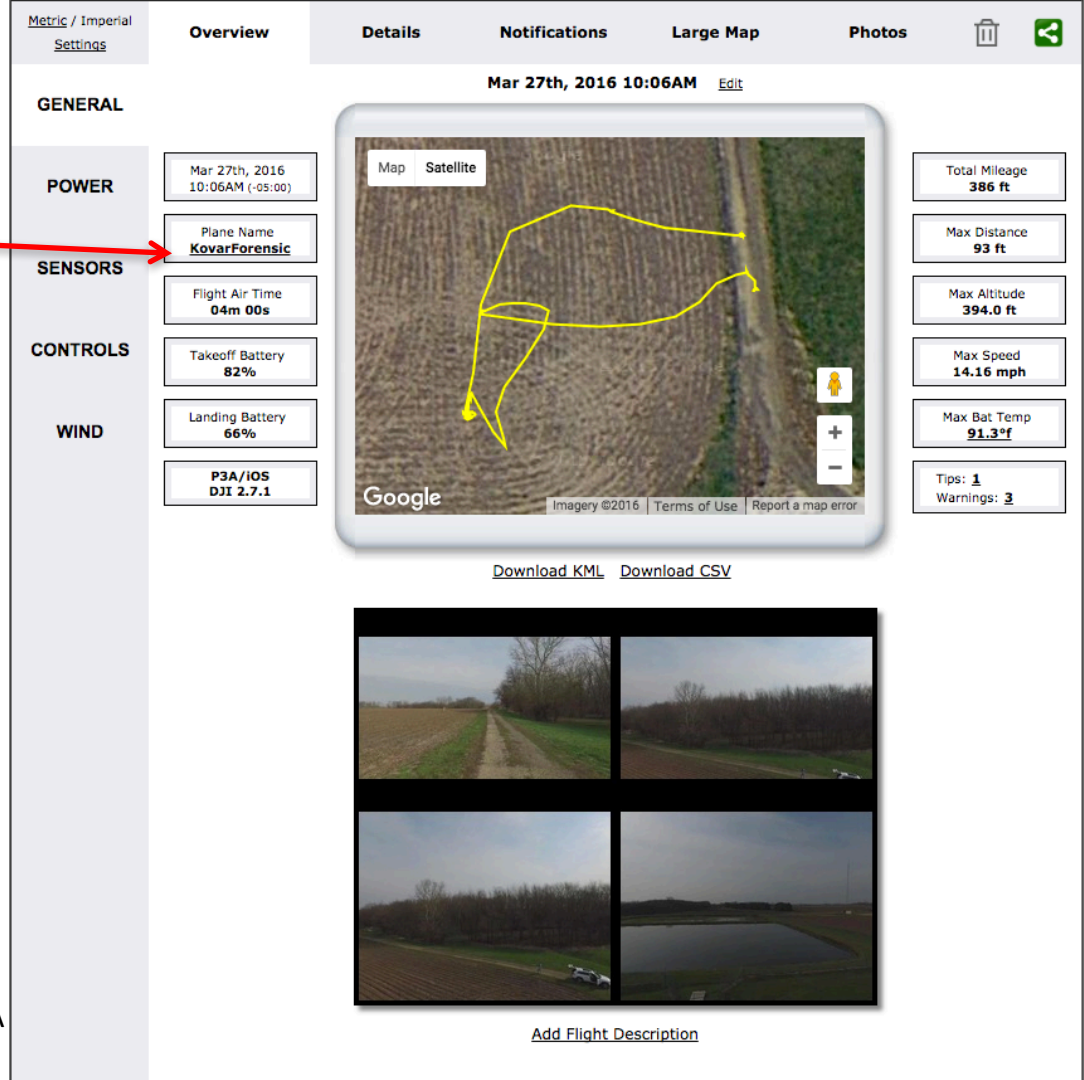
- Photos can be carved manually with Winhex
  Header: 0xFFD8FFE000104A464946
  EOF: 0xFFD9
- All of the JPG files are together at the bottom of the file
- Still dissecting the data fields

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



DJI Flight Record

- Offline Free analysis tool
- TXTlogToCSVtool by ferraript

http://www.phantompilots.com/threads/tool-win-offline-txt-flightrecord-to-csv-converter.70428/

- Again, you will get the .csv and the photos
- This tool was developed for files created on Android devices so iOS created files may be slightly different

Getting the Files

- Image the SMART Device as you normally would to get the .txt files from the app
- Open the UAV, remove the microSD Card and Image
- The UAV may also be put in Flight Data Mode
- Show the mount for Mac

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

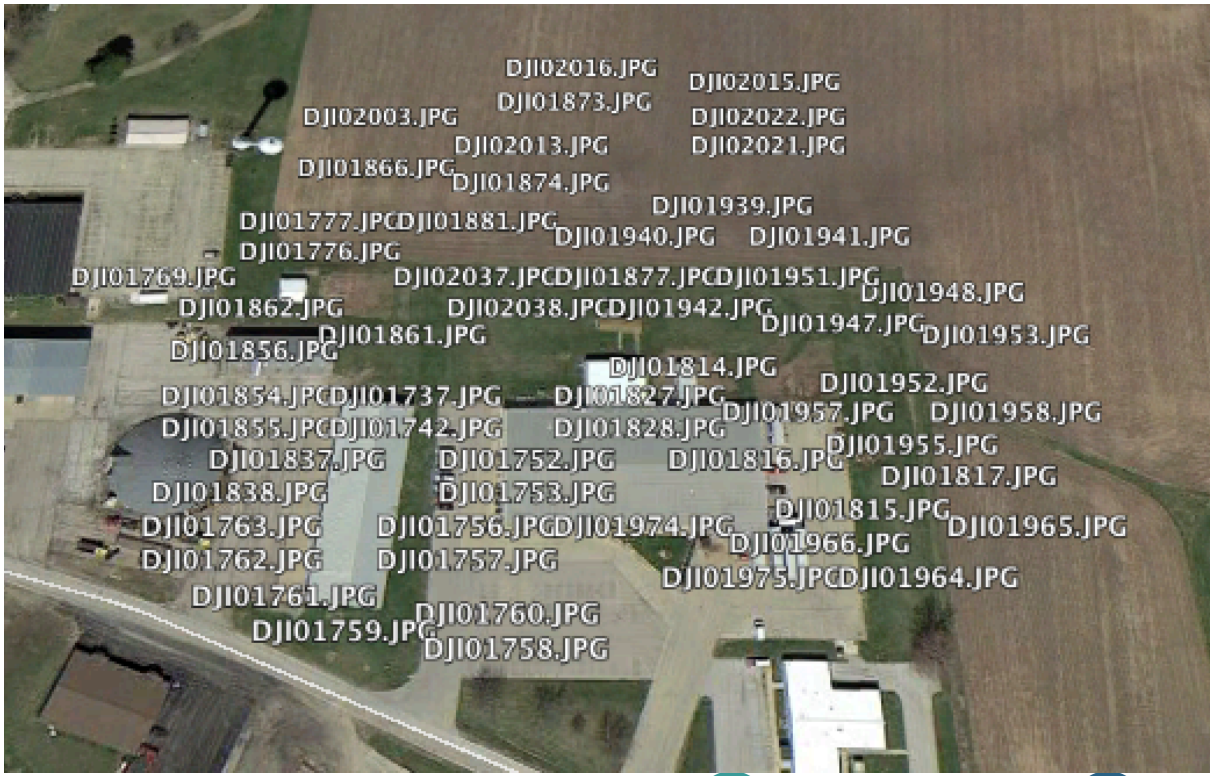
Sensors – EXIF Data

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 ~~do not~~ 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?

Evidence Beyond the UAV

June 5-8, 2016 Myrtle Beach, SC USA

Techno Security & Forensics Investigations Conference

Mobile Forensics World

UAS Exam – Launch Point Evidence

Ground Control Station

- Often a mobile device combined with a radio controller
- Vendor applications and community developed
- Looking for:
  - Default settings
  - Launch points, dates
  - Owner name, account

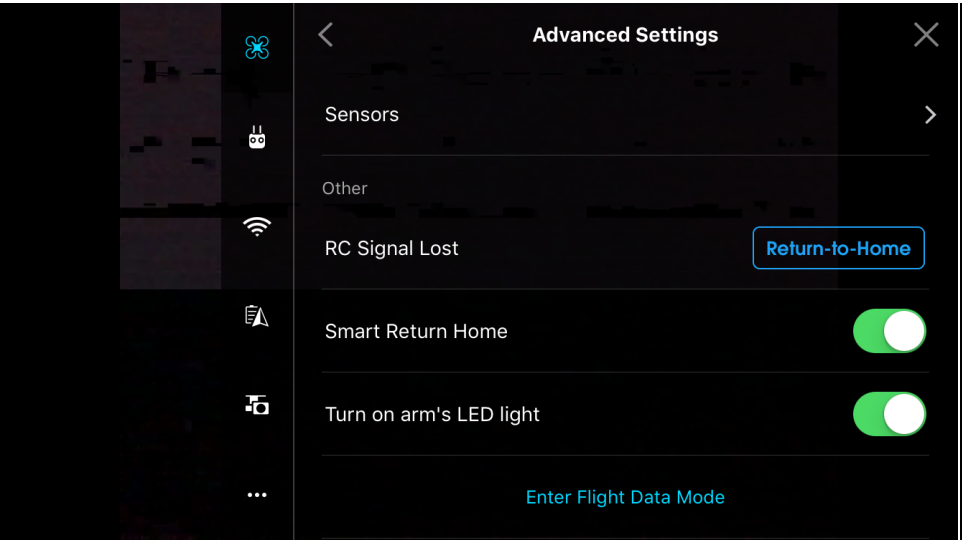
Other Items

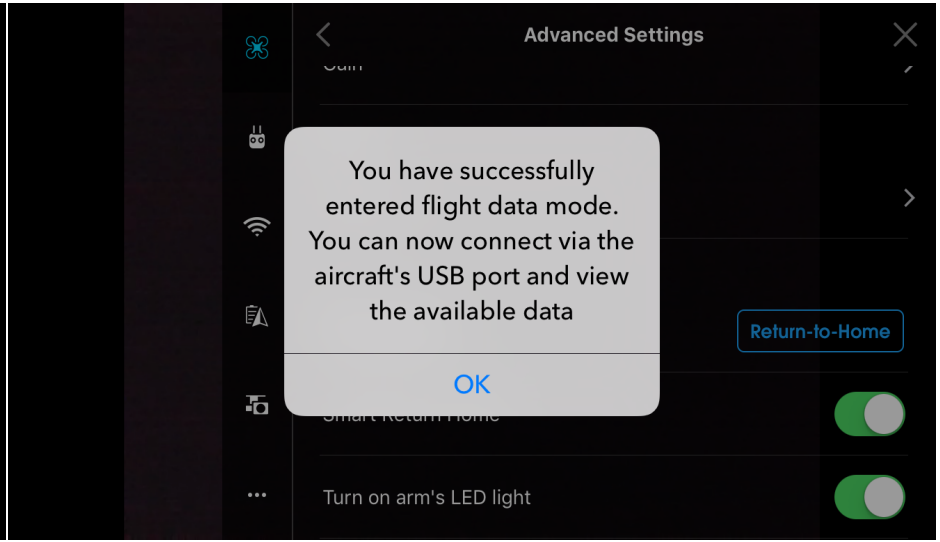
- Spare removable media
- Other UAVs
- Laptops, cell phones, tablets

DJI GO.app Flight Data Mode

- You need the UAV, The RC and a device with the DJI Go.app
- Once all 3 are connected go to the Advanced Settings section of the GO.app
- Select Flight Data Mode

DJI GO.app Flight Data Mode





DJI GO.app Flight Data Mode

- Once in FDM you can connect UAV to a PC
- Yes, you will want to use a USB Write Blocker
- The UAV will mount and you can image the microSD card with your choice of tools
- While the UAV is in Flight Data Mode it will beep and it is loud

DJI GO.app Flight Data Mode

- If you do not have a USB write Blocker you can direct connect
- Just make sure you document your actions.
- To get the FAT32 microSD card to mount in Mac OS X use the command line:

sudo hdiutil attach /dev/disk1s1 -shadow ~/Desktop/shadow

- No matter how you connect the UAV to a computer the transfer will be very slow (approx USB 1.1 speed)
- It will take an hour to image the 4GB micoSD card

UAS Exam – Ground Control Station

Application configuration files contain interesting information

Drone Deploy:

- ajs_user_id
- %22dkovar%40kovarllc.com%22

Pix4D:

- 2016-03-27 10:34:03 [V] [WaypointCustomMissionDJI3::87] create wp at (4x.xxx689,-8x.xxx918) 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

- <string>**03Z0303948**&02.04.10.07</string></plist>com.facebook.sdk:serverConfiguration1383125992006153 -
  <62706c69 73743030 …>

statistics.db

- {user=Anonymous&apptype=0&appversion=2522&**devicetype=2**&deviceversion=01.07.00.00&devicesn=7130333511&productype=3&createtime=1459090198.971318&guid=F7F0A647-B460-41AD-B876-AD971E6079C1
- {user=Anonymous&apptype=0&appversion=2522&**devicetype=1**&deviceversion=02.04.10.07&devicesn=**03Z0303948**&productype=3&createtime=1459090197.770736&guid=A8B53105-8B50-4F36-AAC9-3C5C09D5023D
- {user=Anonymous&apptype=0&appversion=2522&**devicetype=0**&deviceversion=01.22.40.95&devicesn=04CLA51862&productype=3&createtime=1459090196.597396&guid=9C244F41-6F0A-4767-9930-78C74CED66FFÅ;
- {user=Anonymous&apptype=0&appversion=2522&**devicetype=2**&deviceversion=01.07.15.01&devicesn=5443003511&productype=3&createtime=1459095943.455033&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.

We've traced the UAV back home

UAS Exam – Home & Office Evidence

Maintenance, logging & business systems

- Flight and maintenance logs, often with date/time/location/aircraft
- Client & accounting data

Data analysis system

- If not cloud based, this will have a lot of disk, CPU, and RAM
- Historical sensor data

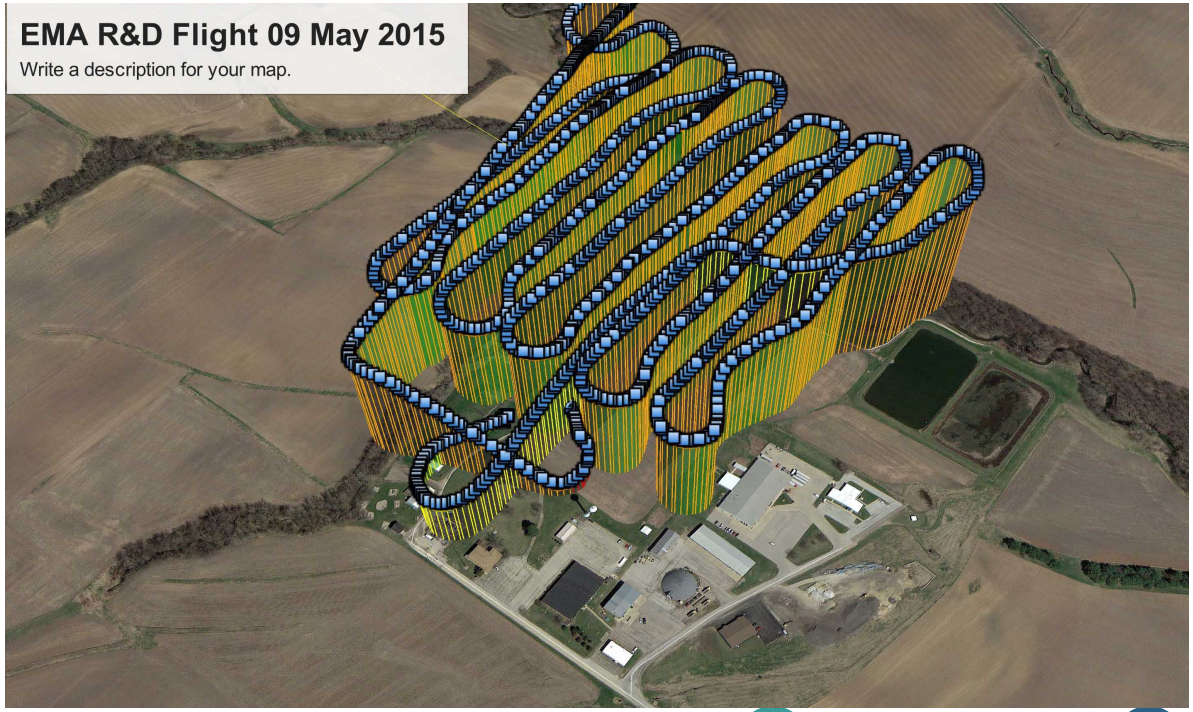
Other

- UAVs, spare parts
- Spare removable media
- Other GCS

Analysis of Other UAVs

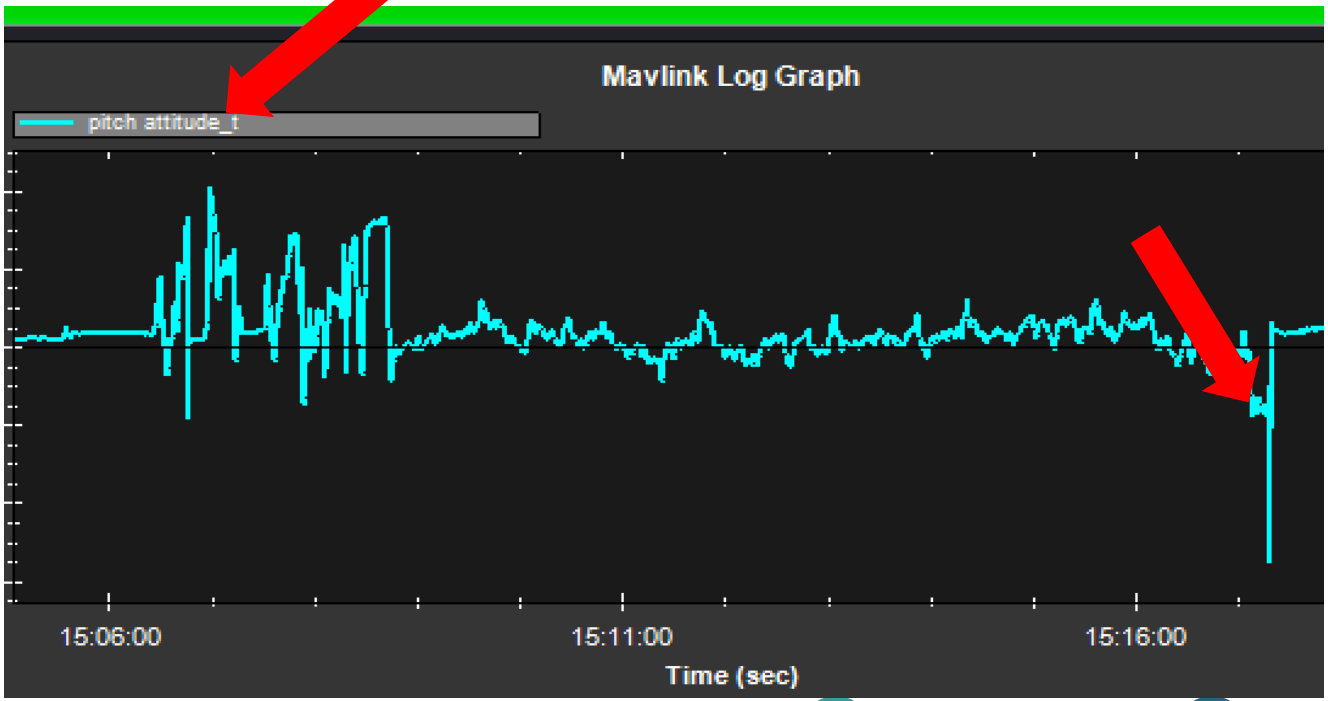
UAVs with PixHawk Flight Controller

The following was created in under two minutes using Mission Planner



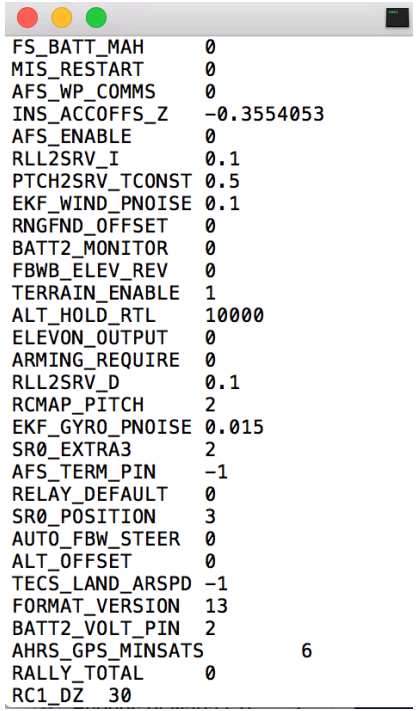
UAVs with PixHawk Flight Controller

And this is what a crash looks like ….



UAVs with PixHawk Flight Controller

And all flight parameters are easily collected



```
FS_BATT_MAH      0
MIS_RESTART      0
AFS_WP_COMMS     0
INS_ACCOFFS_Z    -0.3554053
AFS_ENABLE       0
RLL2SRV_I        0.1
PTCH2SRV_TCONST  0.5
EKF_WIND_PNOISE  0.1
RNGFND_OFFSET    0
BATT2_MONITOR    0
FBWB_ELEV_REV    0
TERRAIN_ENABLE   1
ALT_HOLD_RTL     10000
ELEVON_OUTPUT    0
ARMING_REQUIRE   0
RLL2SRV_D        0.1
RCMAP_PITCH      2
EKF_GYRO_PNOISE  0.015
SR0_EXTRA3       2
AFS_TERM_PIN     -1
RELAY_DEFAULT    0
SR0_POSITION     3
AUTO_FBW_STEER   0
ALT_OFFSET       0
TECS_LAND_ARSPD  -1
FORMAT_VERSION   13
BATT2_VOLT_PIN   2
AHRS_GPS_MINSATS         6
RALLY_TOTAL      0
RC1_DZ   30
```

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

The UAV is paired with controller

&

The UAV is also paired with ground control station

Means unique IDs

Means forensic evidence linking devices

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

Future Work

- Develop stand alone versions of all tools
- Further JTAG analysis
- Further file analysis using above tools
- Facebook and other social media integration
- Other platforms
- Staying current

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:**
- **UAVehicle. 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