CHAMPLAIN COLLEGE

Assignment Title: Drone Forensics

By:

Phillip N Kittelson

Phillip.kittelson@mymail.champlain.edu

By submitting this assignment, I acknowledge that I have read and agree to abide by the Champlain College Academic Honesty Policy. I declare that all work within this assignment is my own or appropriately attributed. I accept that failure to follow the academic honesty policy may result in a failure grade, or expulsion from Champlain College.

Date Due: 04/21/2019

Date Submitted: 04/21/2019

Abstract

Drone technology has advanced significantly within recent years, and has become commercially widely-available. Criminals and terrorist have adopted drones in their operations, and have used drones to deliver explosives, contraband and weapons. Drones can offer much in the way of physical and digital artifacts to an investigator. While providing useful, investigations involving drones bring their own issues and limitations. An investigator needs to be aware of the potential for location, flight and even cloud-base data when performing an investigation.

Drone Forensics

Drones have advanced significantly, especially within the last few years, and have become widely-available for both public and private use. According to the Federal Aviation Administration (FAA), the United States has 1 million registered drone users with an estimated 2.5 million drones flying annually and forecasts seven million drones will be in use in the United States by the year 2020 (FAA, 2018). The drone market has also seen a saturation of over 30 different drone manufacturers with over 100 commercially available models offered. As drone forensics and artifacts are discussed in this paper, the DJI Phantom 3 will be the primary example. This drone comprises most of the lion share of the commercially available drone market.

Uses of Drones

The significant boost in drone technology, and widespread commercial availability of these devices has allowed government agencies, military services and private citizens to take advantage of drone technology with applications in almost everything from surveillance, farming and product delivery. Like most advances in technology those seeking to commit criminal activity have also adopted the technology and have incorporated drones into their operations.

Terrorist groups, such as the Islamic State in Iraq and Syria (ISIS), have developed sophisticated aerial release platforms attached to drones which can be used to deliver unexploded ordnance onto Iraqi and other allied troops. This type of attack is stealthy, low-cost and degastating. Videos are available on the internet showing how accurate these systems are for a trained drone operator.

These tactics have catapulted drones to the number one threat to United States military units and installations in the Middle-East. However, this threat exists in more places than Iraq and Afghanistan (Vocativ, 2017).

In 2018, rebels staged an assassination attempt against the President of Venezuela using drones equipped with explosives. The rebels, though not successful, showed how drones can be used to quickly attack what would have been described as a “hardened” target.

Further north, there are documented instances of Mexican drug cartels using drones to conduct surveillance on United States Customs and Border patrol agents. The cartes use this surveillance to assist drug-loaded land crossers with crossing the border undetected. Additionally, the cartels have also used drones to deliver small packages containing drugs and or weapons across the United States-Mexico border (Giaritelli, 2018).

Like terrorist and organized crime, such as the drug cartels mentioned earlier, drone technology has been adopted by individual criminals. The applications for drones in criminal activity is only limited by the ingenuity of the suspects.

Types of Crimes

Beyond future applications for criminal drone use, we know of several ways drones have been used in the present day.

Most criminal drone activity consists of no-drone and no-fly zone violations, which in the United States are regulated by the FAA. No-drone zones have been established around facilities such as airports, military bases and other national critical infrastructure (FAA, 2018).

Washington D.C., for example, has the most restricted airspace in the United States. Security measures for the Ronald Reagan Washington National Airport include a 15-mile no-drone zone immediately around the airport. Beyond this zone is an additional 15-mile restriction on drones operating above 400 feet. This area more than coverst the National Capital Region.

Military bases and national critical infrastructure, such as dams and power plants, also have no-drone zones established around them. An attack by drone on a public utility provider facility can cause havoc to civilian population centers by knocking out power-generating capabilities.

The dangers from drones are not solley and American issue as well. London's Heathrow Airport shut down for just over 24 hours due to drone activity in its airspace. This incident caused thousands of flight cancellations and a massive unrecorded loss of economic activity.

While these zones are permanent, temporary zones can also be established at large venues such as sporting events and other gatherings. Security measures for the 2019 Super Bowl was even more restrictive than the measures around the nation's capital, and included a 30-mile no-drone zone established by the FAA. Leading up to the event, dozens of drones were seized by the Federal Bureau of Investigation (FBI) for no-drone zone violations. Most of these violations were of amateur drone operators attempting to get a birds-eye view of the venue prior to the big game, however, all instances have to be investigated and taken seriously.

Other events and circumstances may warrant establishment of drone restrictions as well. Drones around wildland firefighting activities is also heavily regulated. Drone use in these areas can, and has, prevented firefighting efforts and put lives and equipment in danger.

Hurricane zones are also restricted to drones because of the danger involved with being outside during a hurricane.

Other crimes involving drones include privacy violations, or stalking. Suspects have used drones to video record residents inside of homes and on other property. Trespassing is also another crime drone operators may commit where a forensic examination can assist with establishing a location for a trespassed person.

In the late 1990's and early 2000's news organizations used to carry live coverage of police activities during hostage and barricaded suspect situations. Suspects realized this as a treasure trove of intelligence and tuned into news coverage of the live situations they created. News outlets have since limited streaming the activities of authorities during these situations, however, suspects have gained the ability to perform surveillance themselves. Surveillance of police activity by drones is a huge concern. Suspects have used drones to spy on police staging around buildings. Police in Japan have seemingly mastered anti-drone practices fighting against organized crime in that country (Henningan, 2018).

Issues With Investigating Drone Activity

Conducting investigations involving drones brings unique issues, situations and limitations to investigators. Drones are very much considered part of the Internet of Things (IoT), and investigators must adhere to federal and state laws and regulations regarding the capture, seizure and analysis of drones, other computer systems and their associated peripherals. These laws include the Wiretap Act with intercepting communications between drones and connected device. Special considerations must be given to jurisdiction, the venue, statute of limitations and the potential involvement of juveniles (DOJ, ukn date).

The first notable issue, and the most important, when investigating drones includes the capture of device and peripherals themselves. An investigator can not analyze what one does not possess. No suspects, or even person's of interest, have been found as a result of the Heathrow Airport incident due to an inability capture the device used in that situation.

To capture a drone, there are three separate methods. The first consists of a kinetic capture.

Kinetic capture involves moving, or mechanical, means to capture a drone. Simply shooting a drone down with a shotgun is an example of a kinetic capture. Other, specialized, shotgun rounds, such as the SkyNet round employed by the United States Air Force (USAF) at their installations around the Middle-East can also be used to effect a kinetic capture. This round deploys a net which is used to envelop the drone and entangle the rotor blades of drones preventing further flight. This employment is only effective at short distances of less than 100-feet due to the limitations of the deployed net.

Potential problems involved with a kinetic capture include causing an uncontrolled landing and an insecure recovery location, data loss and the loss of other physical evidence, such as fingerprints. During one example, VTO Labs was collecting drone images to assist investigators. During one of their test flights, they allowed the land owner of the field to shoot a drone during an experiment. After receiving the shotgun blast, the drone increased its altitude and flew off course and outside of the test area. A kinetic capture of this type can endanger both nearby personnel and equipment, especially when faced with an explosives danger by terrorist use of drones.

A second method of drone capture is a non-kinetic capture. Non-kinetic capture lacks a mechanical means of capture, so a drone would have to be overtaken and controlled by a system such as the NINJA System, also employed by the USAF in the Middle-East. This system detects drones within a given geofenced area and attempts to take control of the device. This is impressive, especially given the recently advances in drone technology which include encrypted communication between the drone and ground control stations.

As part of the capture by the NINJA system, an automated process diverts the drone to designated locations where explosives ordinance personnel can clear the device of potential explosives prior to an investigator's examination. The USAF saw the first successful capture of a drone in a real-world situation in late 2018 after many years of testing and fielding the NINJA system. Commercial airports would, not doubt, benefit greatly from this kind of system, preventing events such as the Heathrow Airport situation.

A non-kinetic capture includes a controlled landing and recovery location, which is also less-likely to result in damage and lost data for an investigator to analyze. This will, however, add flight data to the drones logs at, and post, take-over of the device. This is easily worked around by analysing flight logs and keeping a list of the GPS coordinates for recovery locations.

The third method of seizing a drone is when the drone is not in operation, mostly through routine investigation or through a search conducted on a suspect's premises, vehicle, or other location. While this does not necessarily involve forensic means, all necessary steps should be taken to obtain all drone parts and peripherals to complete a comprehensive analysis.

Other issues with performing drone investigations include the analysis of data formats. Most drone log formats and systems are proprietary in nature and differ from manufacturer to manufacturer. Some of these formats are obfusticated, and encoded, with more recent examples include encryption of data types.

Drone artifacts can be analyzed using open-source programs such as Autopsy, third-party commercial software such as Access Data's EnCase, or even programs provided directly by the drone maker. Manufacturer provided software is often geared towards troubleshooting devices, however, can be used by an investigator. Other tools include software packages developed by some security researchers who have created their own drone log parsers such as the DRone Open source Parser (DROP). The Department of Defense's Cyber Crime Center (DC3) has also produced a drone log parser intended for its investigators. As you can see, the forensic community, private and public, are taking drone involvement in crimes seriously.

Physical Evidence and Artifacts

Investigating drones brings with it both physical and digital evidence for an investigator to collect and analyze.

The primary piece of physical evidence an investigator will handle during an analysis is the drone itself. Non-data evidence on a drone can include fingerprints and DNA left by drone operators. A through collection of this type of evidence needs to occur prior to any disassembly and in coordination with physical forensic specialist.

Drones can be easily disassembled, when necessary, to access internal components such as the on-board SD card, microcontrollers antennas and other ports. Tools necessary include:

- T4 flathead screwdriver
- J00 phillips screwdriver
- 2mm hex head driver
- PH000 screwdriver
- T8 screwdriver
- Plastic pry tool
- Soldering iron (optional for removing components conducting off-chip analysis)

Complete breakdown instructions, including pictures and videos, can be found by requesting access to the National Institute of Standards and Technology's (NIST) Computer Forensic Reference Data Sets (CFReDS) Project through VTO Labs, the contractor responsible for managing the repository. Reports on major models and forensically sound images of can also be downloaded through the repository for further tools testing and analysis.

The chips and other hardware used in drones can vary by manufacturer, and even widely differ within the same model of drone. DJI Phantom 3 contains a 32 bit MCU made from STMicroelctornics, and boasts 128 KB of memory. A 4 GB SanDisk SD card with logs is also on-board.

This SD card can be obtained in a "non-intrusive manner," however, requires the controller to be present and connected and a smart-device prior to being able to access the flight logs via a computer.

The main board for this model also has two chips. The first chip is a Atheros MIPS processor and the second is a 256MB Arduino Micron.

Accessing these chips can be somewhat tricky. Take the Serial Wire Debug (SWD) Pinouts on the mainboard which allows interfacing with one of the chips. If a connection is established using an emulator, as VTO labs discovered, the contents of the entire chip are erased. Thankfully, use of a "savebin" command on the interface recovered the data. Events such as these should be thoroughly documented in notes and reports, explaining the exact steps take to recover data.

All-in-all, the DJI Phantom 3 contains three separate areas of memory storage including the:

- External microSD card
- Internal microSD card
- eMMC component, located on the drone's main circuit board

The external SD card can be acquired through logical means and contains a single FAT32 partition which holds two folders labeled "DCIM" and "MISC." Based on the folder names, these folders are designated to hold any photo or videos taken by a proprietary camera system.

The internal microSD card can also be accessed logically and contains a single FAT32 partition with a "root" folder. This folder contains "FLYXXX.DAT" with flight data.

The eMMC component chip has 128KB of memory and can only be accessed using an a chip-off physical means.

Associated pieces which also need to be collected include rechargeable battery units and sensors.

Rechargeable battery units can display the number of charges completed on the unit and potentially a power level. This can help investigators determine if a drone has been used and how often it is used with the number of recharges. These functions are largely used to help determine the useful life of a battery unit. Not all models support these features, especially the lower-priced models.

Phantom 3's battery circuit board holds two Texas Instruments chips, and may be of future forensic relevance as more techniques are developed.

The presence of a sensor can also help an investigator determine the intended use of a drone device. Sensors can include Light Radar (LIDAR), optical, Night Vision InfraRed (NVIR), thermal, WiFi and Geolocation Positioning Systems (GPS).

LIDAR is a tool used by surveyors to take high-resolution images of topography and larger areas. These are mostly used in a professional setting, and are less likely to be equiped by an ameateur operator.

Optical sensors, such as a camera, are the primary senor used by most done operators. The most common camera systems are GoPros, the proprietary drone manufacturer such as DJI and Sony. These cameras can contain SD cards or stream them using WiFi.

NVIR systems are used for low-light, or night-time video and or photography. The presence of NVIR sensors may point to the time-of-day a drone may have been used.

Drones equipped with WiFi are capable of streaming video, and sometimes audio, to a Ground Control Station (GCS) or other smart-device.

A GCS can range from basic remote control units, which are not capable of receiving data, to smart-devices or other connected devices.

Most typical controllers will not hold any pertinent data beyond serial numbers, as shown by the fact the DJI Phantom 3's controller contains not flash memory. Other ground controllers require smart-device connectivity through apps.

The varied locations and types of data available during a drone forensic analysis vary greatly, and this emphasises the importance of collecting all drone peripherals as part of the investigation.

Digital Evidence and Artifacts

After collection of physical devices, an investigator can collect and analyze digital evidence associated with a drone and its peripherals.

The first artifact an investigator should look for when analyzing a drone are serial numbers. Most devices have more than one serial number. These serial numbers are usually for the drone itself, a serial number for a sensor such as a camera a serial number for rechargeable battery units. These artifacts are important to tie a specific drone, and its peripherals, to a potential suspect.

Drones can also have unique IDs such as master or main controller ID associated with remotely controlling the device. Logs containing these IDs can be recovered from either the drone or the controlling device for those with smart-connection capability.

Additional important drone data includes location and other telemetry data, GPS being the primary of these.

GPS data is largely dependent on the drone model and the flight mode used during the operation of the drone. DJI's Phantom Drone series, as an example, uses several flight modes. These include:

- P-Mode: GPS in use
  - P-GPS: GPS not available, only uses barometer for altitude
- A-Mode: GPS used for positioning only

As shown above, GPS data may not always be available, so an investigator may need to turn to other methods and analyze barometer information if available.

Other GPS location data can include a "Return-to-Home" location of where the drone was first initialized on a particular flight. Most drone models return the drone to this location if communication with the Ground Control Station is lost or interrupted for longer periods or is intermittent. The Return-to-Home feature safety mechanism which may be available to show an investigator where a drone originated from during a specific flight.

Flight data, including vehicle speed, direction and altitude, may also be available for collection. Most of this type of data is USB-exportable. DJI's Phantom 3 flight data is exportable to an application the company makes. This information can also include aircraft status information, with date and time stamps and error messages. Usefulness in any type of investigation largely depends on the data logged by the drone and forensic value would have to be evaluated on a case-by-case basis.

Digital photographs and videos may also be available from a drone, or rather from the drone's sensor. The format for photographs on most of these sensors is usually PNG format, which should be easily examined by an investigator using traditional metadata extraction and examination procedures.

Videos are also stored in common MOV and MP4 formats and drones can generate upto 720P video at 30 frames per second, which also should present easy examination by an investigator. These videos can include date and time stamps and GPS information.

Screenshots from videos are also exportable to PNG format, and can be exported on a smart-device connected to the drone. The Phantom 3 includes a WiFi video link, which streams video to ground stations and smart-devices.

WiFi systems on a drone may be of some use as well to an investigator, and use a 2.4-2.483 GHz antenna with a range of up to 1000 meters depending on the model. Ground Control Stations usually host this connection and have a network Service Set Identifier (SSID) to identify the network. Most of these SSIDs incorporate part of the Ground Control Station's serial number and drone model designation. At this point it is unknown if live packet sniffing can be performed on a drone using its network features. However, this would only be useful during actual operation of the drone and requires equipment setup in advance. Suspects monitoring police activity outside of a hostage situation would likely be the best application for this type of interception within legal limitations.

Digital evidence from a Ground Control Station may also be of use during an investigation. These devices run either open-source or commercial software produced by the drone manufacturer. Logs, and which data is logged, on these devices often depend on the make and model of a drone with some requiring an off-board data logger for collection.

For those Ground Control Stations which do log data, the log on a Ground Control Station is often a single file and extractable for analysis. Other data on the Ground Control Stations may include launch points and date and time stamps.

Some drones have companion applications on app stores such as iTunes or the Android application store or may be directly downloadable via the manufacturer's website, independent of a particular phone makers application store. These apps allow operators to input flight plans, which allow a drone to fly a predetermined route and given altitude. This data can show an operator intended to fly a drone in a particular area. Some drone makers, such as DJI, build-in no-drone zones into their Ground Control Station software preventing this from happening, however, not all systems are impenetrable and not all drone manufacturers take part in this practice.

These companion applications may also include owner name, login and account information,which may be accessible through traditional mobile forensics methods. This information may be used via legal methods to obtain the profile, and other available data, from an owner's account with the drone manufacturer.

Even with all the drone parts and pieces in hand, and investigator should also look for other computer systems as part of their investigation. Desktop and laptop computer systems are often used to store data downloaded from a drone. Computer systems should be seized and analyzed using standard analysis procedures and techniques.

Digital photographs and videos taken by a drone may also be present on a computer system. These artifacts can include metadata and GPS location data as mentioned earlier.

Log files for drones may also be located on a computer system. Some drone manufacturers often design computer-based programs a drone enthusiast can import and analyze log files on to troubleshoot problems which originate while in flight. These programs are often proprietary, but can be used by investigators themselves to conduct log analysis. Often the best tools are made by those who design the devices.

Mapping software, mostly used for commercial solutions and applications, are available and can be present on a suspect's system. Additionally, any backup and saved drone config information should be collected as well for examination. Altered drone firmware can point to the intent to bypass a drone's built-in no-fly zone restrictions.

Other devices an investigator should collect include smart-devices such as phones and tablets. These devices can contain location data, WiFi connection data, digital photographs and videos and drone operator account information in addition to the traditional artifacts contained and used for a regular investigation.

Digital artifacts are not always relegated to the immediate physical world either. Alternate locations of digital artifacts investigators should look for include data stored in the cloud. Cloud data, especially this day-and-age, consists of much of the digital data available and is very prevalent and wide-spread. The potential for cloud-based data in an investigation should always be considered. Cloud-base services are largely broken up into two areas: consumer and commercial.

Consumer cloud data is usually hosted by third-party services or websites and can include sites such as Youtube and Facebook. A suspect's YouTube channel and Facebook page should always be checked for video or photographic artifacts.

Commercial cloud data can include specialized programs or websites such as Drone Deploy, Data Mapper, Airware and other vendor specific services or websites. These services are mostly used for commercial a and should be largely absent when dealing with an amateur drone operator or small-crime suspect.

Data which should also be collected are the credentials used to upload the artifacts to the cloud. Subpoenas sent to these cloud providers can result in additional information relevant to an investigation.

Conclusion

Drone technology has advanced significantly over the last few years. Criminal organizations and terrorist have used drones to further their causes and increase the influence of their groups. An investigator analyzing drone artifacts will have unique issues present themselves during an investigation, and needs to be aware of the potential for the full gamut of evidence which should be captured during an analysis. These artifacts transcend the physical into the digital and traverse into the cloud often. Both commercial and open-source solutions should be explored to deal with the dynamic world of drone technology to work beyond the proprietary nature of the industry and collect evidence in a sound and forensically suitable manner.

References

BBC. (2019, January 9). *Heathrow airport drone investigated by police and military*. Retrieved from BBC News: https://www.bbc.com/news/uk-46804425

BBC. (2019, January 8). *Heathrow airport: Drone sighting halts departures*. Retrieved from BBC News: https://www.bbc.com/news/uk-46803713

Clarke, C. P. (2018, August). *Approaching a 'New Normal': What the Drone Attack in Venezuela Portends*. Retrieved from RAND Corporation: https://www.rand.org/blog/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela.html

DJI. (n.d.). *Phantom 3 Standard Specs*. Retrieved from https://www.dji.com/phantom-3-standard/info

FAA. (2017, April 7). *FAA Restricts Drone Operations Over Certain Military Bases*. Retrieved from Federal Aviation Administration: https://www.faa.gov/news/updates/?newsId=87865

FAA. (2018, December 11). *Airspace Restrictions*. Retrieved from Federal Aviation Administration: https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_restrictions/

FAA. (2018, October 19). *No Drone Zone*. Retrieved from Federal Aviation Administration: https://www.faa.gov/uas/resources/community_engagement/no_drone_zone/

Forensic Focus. (2018, April 23). *Drone Forensics - How To Deal With The New Threat*. Retrieved from YouTube: https://www.youtube.com/watch?v=LfcTViRm2no

Giaritelli, A. (2018, October 31). *Drone activity by drug cartels surges on San Diego's border with Mexico*. Retrieved from Washington Examiner:

https://www.washingtonexaminer.com/news/drone-activity-by-drug-cartels-surges-on-san-diegos-border-with-mexico

Grudo, G. (2017, May 19). *Catching RPAs Using Actual Nets and Other AFRL Innovations at Lab Day*. Retrieved from Air Force Magazine: http://www.airforcemag.com/Features/Pages/2017/May%202017/Catching-RPAs-Using-Actual-Nets-and-Other-AFRL-Innovations-at-Lab-Day.aspx

GÜLATAŞ, İ., & BAKTIR, S. (2018). Unmanned Aerial Vehicle Digital Forensics. *Journal of Naval Sciences and Engineering*, 32-53.

Henningan, W. J. (2018, May 31). *Experts Say Drones Pose a National Security Threat — and We Aren't Ready*. Retrieved from Time Magazine: http://time.com/5295586/drones-threat/

Houck, C. (2017, October 26). *The Pentagon's IED-Hunters Have a New Target: Drones*. Retrieved from Defense One: The Pentagon's IED-Hunters Have a New Target: Drones

Judson, J. (2017, October 20). *'No silver bullet': Pentagon struggles to defeat drones in cat-and-mouse game*. Retrieved from Defense News: https://www.defensenews.com/digital-show-dailies/ausa/2017/10/20/no-silver-bullet-pentagon-struggles-to-defeat-drones-in-cat-and-mouse-game/

NIST. (Drone Data Set). *Drone Data Set*. Retrieved from Computer Forensic Reference Data Sets (CFReDS): https://www.cfreds.nist.gov/drone-images.html

Northrop Grumman. (2016, October 4). *Northrop Grumman Demonstrates Counter-UAS Technologies at Black Dart Exercise*. Retrieved from Northrop Grumman News Room: https://news.northropgrumman.com/news/releases/northrop-grumman-demonstrates-counter-uas-technologies-at-black-dart-exercise

SANS. (2015, July 28). *Forensic Analysis of sUAS aka Drones - SANS DFIR Summit 2015*. Retrieved from YouTube: https://www.youtube.com/watch?v=36rZy9V_avo

SANS. (2016, Nov 28). *UAV Forensic Analysis – Next Gen - SANS DFIR Summit 2016*. Retrieved from YouTube: https://www.youtube.com/watch?v=LpMmaxlSCLQ

UNH Cyber Forensics Research & Education Group. (2017, December 23). *Drone Parser (DROP)*. Retrieved from Github: https://github.com/unhcfreg/DROP

Vocativ. (2017, Nov 4). *ISIS Propaganda Video Drops A Bomb From A Drone*. Retrieved from YouTube: https://www.youtube.com/watch?v=cz2jrmnm7ds

Voidsec. (n.d.). *A Drone Tale*. Retrieved from Voidsec: https://voidsec.com/a-drone-tale/

Voidsec. (n.d.). *Hacking the DJI Phantom 3*. Retrieved from Voidsec: https://voidsec.com/hacking-dji-phantom-3/

VTO Labs. (2017, October 10). *Behind The Scenes with VTO - Drone Forensics*. Retrieved from YouTube: https://www.youtube.com/watch?v=XQFuTcA_Lk8