International Journal of Digital Crime and Forensics
Volume 12 • Issue 1 • January-March 2020

Towards a Better Understanding of Drone Forensics:
A Case Study of Parrot AR Drone 2.0

Hana Bouafif, ESPRIT School of Engineering, Tunis, Tunisia
Faouzi Kamoun, ESPRIT School of Engineering, Tunis, Tunisia
Farkhund Iqbal, College of Technical Innovation, Zayed University, Abu Dhabi, UAE

ABSTRACT

Unmanned aerial vehicles (drones) have gained increased popularity as their innovative uses continue to expand across various fields. Despite their numerous beneficial uses, drones have unfortunately been misused, through many reported cases, to launch illegal and sometimes criminal activities that pose direct threats to individuals, organizations, public safety and national security. These threats have recently led law enforcement agencies and digital forensic investigators to pay special attention to the forensic aspects of drones. This important research topic, however, remains underexplored. This study aims to further explore drone forensics in terms of challenges, forensic investigation procedures and experimental results through a forensic investigation study performed on a Parrot AR drone 2.0. In this study, the authors present new insights on drone forensics in terms of forensic approaches, access to drone's digital containers and the retrieval of key information that can assist digital forensic investigators establish ownership, recuperate flight data and gain access to media files.

KEYWORDS

Drone, Drone Forensics, Forensic Investigation, UAV, Unmanned Aerial Vehicle, Unmanned Aerial System

INTRODUCTION

Unmanned aerial vehicle (UAV a.k.a. drone) is a remotely controlled aircraft. It is capable of capturing images and video sequences of a targeted region and transferring them to a remote server for storage and further processing. The server can be co-located with the Ground Control Station (GCS) or it can be housed in a secured cloud environment. A drone is usually controlled by a handheld device such as a radio controller, a mobile phone or a tablet (Singh, 2015).

The past few years have witnessed a steady proliferation of drones across a wide spectrum of applications including recreational, commercial, educational, law enforcement, and national security uses. Business Insider (BI) Intelligence expects sales of drones to surpass $12 billion in the U.S. by 2021 (Camhi, 2016). Today, drone technology is no longer confined to high-end military and meteorological uses. In fact, small UAV toys, which are capable of capturing live videos and images, can be purchased today for few hundred dollars from various toy retailers (Hyde, 2014). In the consumer market, major players like 3D Robotics, Parrot and DJI are constantly expanding the usefulness of their UAV product lines with new features, better performance and energy efficiency, as well as smaller size, reduced weight and enhanced usability.

DOI: 10.4018/IJDCF.2020010103

Recent advances in embedded systems, nanotechnologies, sensor technologies, image processing and navigation systems have given rise to a new breed of affordable UAVs with powerful information collection, storage and processing capabilities. The UAV hobby community is also booming and various online blogs and forums have been established to support customized usage of drones.

The Intelligence, Surveillance, and Reconnaissance (ISR) features of UAVs have enabled a myriad of new applications and uses of these devices that go beyond the recreational uses (Ravich, 2015). In fact, when equipped with sophisticated algorithms for information acquisition and processing, UAVs can retrieve a rich set of information footages including high resolution images and videos, thermal images, and accurate 3D topographical maps, among many others. Accordingly, UAVs have been used in various tasks such as film making, ecosystem monitoring, precision irrigation, parcel delivery, border patrolling, crowd monitoring in major events and identification of hazardous material. Added to this, they have been implemented in search-and-rescue operations, damage assessment and cetera (Singh, 2015).

Unfortunately, UAVs can as well be used to launch illegal actions, including voyeurism, invasion of the privacy of citizens and sensitive places, smuggling of contraband items, spying on individuals or other nation states. This usage may include also espionage on companies and government entities, and the unauthorized launching of aerial missile attacks. In the recent past, drones have also been caught in unintended violation of no-fly zones. Today, there is a growing fear that they might be used by terrorists to perpetrate panic or cause other damages (Elands et.al, 2016).

The past few months have witnessed an increasing number of reported "illegal" usages of drones, including commercial usages that violate FAA regulations, unlawful surveillance and drug smuggling, among many others. Thiobane (2015) argued that drones are targeted by criminals for their payload value, and their capabilities to launch data breach and cyber-attacks. For instance, on October 2015, a Tulsa man was accused of using a drone to smuggle contraband items to an Oklahoma State Penitentiary inmate with Tulsa gang ties (Pickard, 2016). On July 2015, the Pakistan army claimed that digital forensic tests on a Quadcopter it downed along the line of control (LoC) revealed that the device originated from India. TV media have also reported drones' violation of restricted airspace around nuclear submarine site and air navigation orders at major sporting events, and the catching of abandoned UAVs at the White House lawn (Kovar, 2015). Many other drone-related incidents have been reported in the press, including the usage of drones to smuggle drugs over the US/Mexico border, and the flying of drones over restricted and controlled airspaces such as the airports. The potential criminal usage of drones will be further amplified as these devices continue to evolve with a new breed of embedded devices and capabilities.

Drones have the capability to relay video imaging, launch cyber-attacks, jam, hack or spoof the wireless communication links of surveillance, public safety and security devices (Hyde, 2014; Elands et.al, 2016). For example, Paganini (2014) reported that the Snoopy application, running on a drone, can detect the presence of a nearby mobile phone and tricks its owner that s/he is connecting to a trusted access point, which can potentially lead to identity theft attacks. Drones are also vulnerable to cyber security attacks (e.g., jamming, spoofing, hacking, and eavesdropping) that can lead to hijacking, theft of collected information, and loss of control (Elands et.al, 2016).

The illegitimate uses of drones led many law makers, civil groups, law enforcement agencies, aviation regulators, and governments express their deep concern over the potential unlawful and criminal usages of these devices. This concern is further amplified by the fact that UAVs are accessible to almost anybody at any location at every price point and at any time (Ravich, 2015). The past few years have witnessed a rapid growth in the number of startup companies with innovative technologies and applications for drone usage and many people are becoming skeptical about the future landscape of drone usage (Elands et.al, 2016). When not properly controlled, or when operated during bad weather conditions, drones have been involved in many incidents involving collisions with manned aircrafts and damages to aircrafts' engines (Elands et.al, 2016). A malfunctioning drone can crash over persons and properties on the ground, resulting in potential physical damages and injuries.