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.

In the U.S, the Federal Aviation Administration (FAA) bans the flying of private, civil (non-governmental) and commercial UAVs, unless it is pre-approved either through a Special Airworthiness Certificates – Experimental Category (SAC-EC) for civil aircraft for the purpose of R&D, crew training, and market surveys. It can also be approved in advance via petitions to the FAA for exemption under restricted category or for commercial use in low-risk controlled environment.

The potential misuse of drones to launch illegal or criminal activities led forensic analysts to pay special attention to the forensic aspects of these devices. In fact, a captured or abandoned UAV (or its remains) can reveal a rich set of uncompromised digital evidence that can be used to support civil and criminal lawsuits.

Drone Forensics can be viewed as a subset of Mobile and Wireless Forensics which belongs to the wider category of Digital Forensics (Singh, 2015). Traditionally, digital forensics has focused on extracting evidences from conventional computing devices such as mobile phones, computers, tablets, or digital cameras because the pervasive usage of these devices makes them more likely to be used by criminals (Hyde, 2014). However, as explained in the next section, the unique combination of a drone's hardware artifacts and software containers makes drone forensics a big challenge. New investigation frameworks and tools are now required for both forensic investigators and digital forensic researchers to facilitate the forensic investigation of UAVs. However, literature reveals that research on drone forensics is still in a premature stage reflected by the lack of in-depth understanding of drone forensics challenges, and the scarcity of sound drone forensics investigation procedures and results.

The objectives of this contribution are threefold: (1) draw the attention of researchers to the key challenges of drone forensics, and seek a better understanding of some of these challenges through a case-study related to the Parrot AR drone 2.0, (2) present a drone forensic investigation procedure that can guide future research and (3) provide new results on drone forensics including the ability to access the file system from FTP or serial connections as well as the retrieval of the controller's Android ID that can be used to establish ownership.

The remaining of this paper is organized as follows: In Section 2, we present a literature review and highlight the contribution of this study. In Section 3, we discuss key challenges in drone forensics. Section 4 presents our research methodology. In Section 5, we present some experimental results on the forensic analysis of Parrot AR 2.0 drone. Finally, in Section 6, we provide a summary of the main findings of this study and some recommendations for future research.

LITERATURE REVIEW AND RESEARCH CONTRIBUTIONS

The recent influx of small-scale digital devices such as smart TVs, smart toys, GPS, gaming consoles, and drones in the market has increased the risks of misusing these devices to launch illegitimate and criminal activities. Therefore, investigating these devices for forensic relevance has become imperative. The literature review indicates that very few studies have been conducted on forensic investigation of gaming consoles (Khanji et al., 2016), smart toys (Rafferty et al., 2017), smart TVs (Hung et al., 2016), and smart meters (Hasan et al., 2018); and drones are not an exception. To date, drone forensics remains an unfamiliar subject to many law enforcement agencies and digital forensic investigators.

Peacock & Johnston (2013) performed a series of experiments to test some security vulnerabilities of the Parrot AR drone 2.0. They found that the drone had some open ports (enabled by default) that could be accessed by a third party. Their study also revealed that the Parrot could be de-authenticated, thus suggesting that the control can be hijacked by an unauthorized device.

Among the most notable earlier research contributions on drone forensics is the study of Horsman (2016) which was based on the Parrot Bebop drone. The author presented an introductory discussion on UAV forensic analysis and highlighted various challenges associated with drone forensics analysis. Recently, Clark et al. (2017) presented some preliminary results of a forensic analysis on the DJI Phantom III drone with a particular focus on analyzing the proprietary files structures stored by this particular drone. The authors proposed a tool to parse the proprietary DAT files format of the

Phantom III. By correlating data extracted from the mobile device and the drone, the authors were also able to link the user to a particular drone. This, of course, assumes that both the drone and the controller are available.

This study aims to enhance our understanding of drone forensics by drawing the attention of forensic investigators and researchers to the peculiar challenges associated with this research field. Our study suggests that drone forensics can be integrated into the broader digital forensic discipline to the same degree as other computing devices. Put differently, our research suggests that, in principle, the same standard forensic investigation procedures and workflows that apply to information retrieval from computers, cameras, mobile devices, smart TVs, or gaming consoles can be adapted to drone forensics. We present a drone forensic investigation procedure and provide some new results of a forensic investigation on a Parrot AR drone 2.0 that address some of the important issues raised by Horsman (2016). It should be noted that our work is limited to the Parrot AR drone 2.0 and, as highlighted by Clark et al. (2017), trying to develop a generic approach to forensically analyze all types of drones available on the market is an intricate and an exhausting endeavor.

CHALLENGES OF DRONE FORENSICS

Performing a thorough forensic analysis on drones can be a daunting challenge for digital forensic investigators for the following main reasons:

- The components of a small unmanned aerial system (sUAS) (e.g., drone, radio controller, server) which constitute the physical evidences can be potentially scattered in various locations. Further, establishing a sound forensic association between a seized drone and the associated radio controller to ascertain ownership can be challenging (Horsman, 2016).
- The versatility of the digital containers embedded in a typical UAV aircraft makes it difficult for the digital forensic analyst to rely on a single forensic tool to extract all the information needed for the forensic investigation.
- Performing a forensic imaging of the on-board UAV camera, without jeopardizing its integrity, may not be straightforward in most cases. Many drones provide USB connections that do not allow direct access to the physical disk for forensic imaging (Horsman, 2016). This forces forensic investigators to rely on wireless connections to perform forensic imaging remotely (over a network).
- Some embedded data storage containers (such as the recorded flight data residing in the flight controller chip) can be concealed or access-protected, making it difficult for the investigator to plug in a forensic device and extract the digitized evidence. In addition, as reported in (Horsman, 2016), potential access restrictions can prevent the operating system files and content from being included in the forensic image, forcing the forensic investigators to establish a Telnet session with the UAV and to issue standard commands to browse system folders and configuration files.
- A single UAV aircraft can host more than five different types of file systems. This increases the chance that some of these files would not be supported by existing commercial forensic tools (Kovar, 2015).
- The on-board drone's software, hardware and firmware have not been standardized yet and may vary from manufacturer to manufacturer. For instance, to date there is no defacto standard protocol for flight controllers, nor a standard format for representing flight data. Some vendors rely on proprietary solutions which further complicates the forensic analysis. Users can enhance the functionality of a drone by embedding additional components or by modifying the device using software development kits (SDKs) that are provided by most drone manufacturers.
- Access to the flight data through the on-board flight controller chip often requires explicit owner permission via the remote control, while the remote control would most likely be unavailable for forensic investigators. Further, the flight data, extracted from the flight controller chip is usually

encrypted. Hence the absence of the remote control adds further complexity to the forensic investigation (Elands et al., 2015).
- Similar to other small-scale digital devices, drones rely heavily on volatile memory and the flight data stored therein will vanish if the battery drains out. Further, some sensor data can be programmed to be uploaded to a secure server hosted in a private or public cloud or be posted on file sharing or social networking sites.
- Not all commercial drones have flight controllers that are equipped with data logging capabilities.
- When the controller is not seized with the drone, it might not be possible to ascertain ownership of the drone (i.e., pairing between the seized drone and the controller) based on a forensic analysis of the drone's digital content (Horsman, 2016)
- A suspect can use the controller to remotely delete media files from the drone or perform a complete factory rest, which can jeopardize the forensic investigation (Horsman, 2016).
- GPS information stored in the drone includes the GPS location of the handset controller and the GPS information relating to the drone's flight path. Both forms of GPS information can be tampered using GPS spoofing application, or blocked from being recorded, thus hiding the true drone's flight path or the location of the handset during the flight (Horsman, 2016).

Among the challenges that this contribution aims to address are the assertion of drone's ownership based on the extracted digital content and the intricate task of accessing the file system (which is performed in our case via FTP and serial connections).

Among the drone forensics challenges that this contribution aims to address are:

- Intricate task of accessing the file system (which, in our case, is performed via FTP and serial connections)
- Assertion of drone's ownership based on the extracted digital content

RESEARCH METHODOLOGY

As a first step towards developing sound forensic methodologies and workflows, forensic investigators and researchers need to know on where to look for key pieces of both physical and digital evidence. For this purpose, it is important to note that a typical sUAS consists of the following key components which can be scattered in geographically-dispersed locations:

- The drone: contains radio transceiver module, CPU, internal flash memory, flight controller chip (with possible data logging capabilities), multiple sensors (e.g., optical image sensors, inertial (gyro-meters and accelerometers) sensors, velocity sensors, magnetometers, GPS sensors, etc.), compass, batteries, collision avoidance detectors, spectrometers and spectrophotometers, wireless router, optional mounted camera, removable SD card, engines, QR code, Serial and model numbers, optional small solar panels, and carried payload, among others.
- The Battery charging system.
- A radio controller or typically a smartphone (with a dedicated flight navigation application) acting as a remote controller. Some advanced drones can be controlled with First Person View (FPV) terminals or video goggles for telepresence.
- An optional Wi-Fi range extender.
- An optional laptop that might be used to configure other components.
- A server present at the ground level or in a remote cloud environment, where the captured data can be transferred and stored.

Each of the above components can be used as physical evidence during a forensic investigation.

This study is limited to performing forensic investigation on a specific drone, namely the Parrot AR Drone 2.0 with the main objective of extracting as much forensically relevant information as possible to support the investigation process. Based on the six cardinal points of investigation (5W +1H), drone forensics aims to address the following questions:

- **What** happened? (nature of the offense)
- **Where** did it happen? (place or location of the offense)
- **When** did it happen? (time and date)
- **Who** was involved? (owner of the drone)
- **Why** did it happen? (reason or motive of the offense)
- **How** did it happen? (manner, methods and devices used in the offense)

To address these questions, the investigator needs to extract forensic data related to drone ownership (controller's ID, serial number, Android ID, etc.), path flight history (including location from where the drone was launched, flight attitudes, speed, flight-time and distance traveled), onboard sensors that have been activated, photographs and video recordings, log files, system files, and timestamps, among many others. The goal of the forensic investigation is to validate the requirements of a digital non-repudiation by corroborating the drone's ownership with the evidence of deliberate usage. Forensic investigation on other physical components, including the radio controller and the ground control server, is outside the scope of this paper.

Our drone forensics investigation approach is based on the principle that drone forensics (especially logical acquisition) can be viewed as the consolidation of file carving and forensic analysis, performed on the key discrete digital containers of the drone. They include:

- Embedded OS and associated file systems and firmware,
- Digital camera image files and associated thumbnails or EXIF optical sensor metadata,
- Digital camera video files,
- Telemetry information,
- Flight path data based on flight controller chip information and GPS coordinates.

The research methodology of this study is inspired by the general guidelines for forensically examining artifacts as outlined by NIST Special Publication 800-86 (Kent et al., 2006) and it consists of three main steps:

Step 1: Access with caution the UAV aircraft and ensure that it is powered off to prevent remote tempering of the data. Consider traditional forensic investigation techniques to establish ownership, based on fingerprint and DNA techniques. Ensure that these evidences are preserved throughout the investigation.

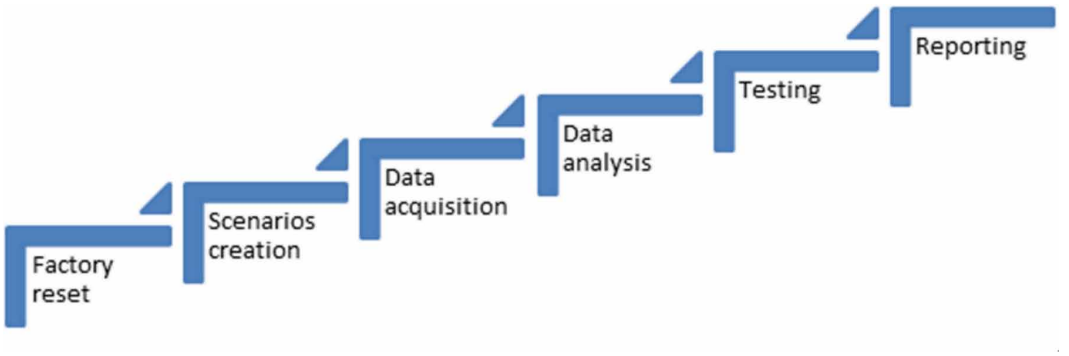
Step 2: Access and document the various artifacts and digital containers, including those stored in the removable SD card. Physical evidences can include the drone's manufacturer, Serial/model number, MAC address, payload, and QR code, among others. Caution must be exerted to ensure the integrity of the digital forensic evidence and hence ensure that the onboard data extracted is forensically validated.

Step 3: Analyze the various artifacts and digital containers to recover evidence: Firmware, thumbnail images and EXIF metadata, Linux file systems, registry settings, active/hidden files, and mount files.

To accomplish the aforementioned steps, we followed a six-phase approach which is depicted in Figure 1.

This approach was inspired from the digital forensic investigation literature including the work of Hoog (2011), Sivakumaran (2014) and the survey paper of Yunus et al. (2011).

Figure 1. Methodology



Phase One: Perform a factory reset on the drone and its controller (the Android smartphone in our case) to clear up configuration settings and old data such as past flight data and video cache from NVRAM.

Phase Two: Install the *AR.Freelight* application on smartphone and create some simulated flight scenarios that include image captures and video recordings.

Phase Three: Switch off the drone and use the disk dump (*dd*) utility to dump the entire disk to an image file. Extract embedded digital evidence that includes flight data, EXIF data in recorded media files and ownership data etc.

Phase Four: Use *Exiftool* to analyze metadata on JPEG and MP4 files. Analyze the *userbox* file which is created each time a flight session is established with the Parrot AR drone 2.0. The *userbox* file contains both configuration details (e.g. firmware version, serial number, total flight time, flight settings) as well as navigation data (e.g. drone status, attitude, speed, sensor data, battery level, GPS details). Analyze additional artifacts and digital containers such as Linux file system, registry settings, path flight logs, and hidden files. Aggregate and correlate the collected evidences to reconstruct events or actions in order to generate initial hypotheses and provide facts.

Phase Five: Conduct experiments to approve or disprove the hypotheses. If the test results do not support some hypotheses, then revise them and perform further tests.

Phase Six: Provide the key findings of the forensic investigation, along with the associated levels of confidence. Further, provide a detailed description of the steps conducted throughout the investigation and document all the information related to the acquisition and the analysis phases. This allows other examiners to understand what has been done and to access the outcomes independently in order to confirm or disprove alibis and provided claims.

CASE STUDY: THE PARROT AR DRONE 2.0

To gain a better understanding of drone forensics, we present in this section the details of a forensic investigation study performed on a Parrot AR drone Power Edition version 2.0 (Figure 2).

The Parrot AR Drone 2.0 (hereafter referred to as the "Parrot AR") is a remote-controlled quadcopter from the French company Parrot SA. The connection to the drone is typically established using its wireless router, which consists of a wireless 802.11 chipset. The Parrot AR can be controlled using smartphones or tablets, running iOS (Freelight application) or Android (AR Freelight) operating systems. Once the connection between the smartphone and the Parrot AR is established, the two devices are automatically paired. The Parrot AR is equipped with a high definition frontal and a vertical camera that provide full-range coverage.

Figure 2. The Parrot AR drone power edition 2.0

The Parrot AR is based on a Linux operating system running kernel version 2.6.32 (BusyBox). It features a 1 GHz 32-bit ARM cortex A8 processor with 1 Gbit DDR2 RAM at 200 MHz. The Parrot AR is equipped with a flight recorder that uses a plug-and-play USB connection with 4GB of built-internal flash memory to store videos and flight data, as shown in Figure 3. The flight recorder can geo-locate and keep track of the position of the Parrot AR with its GPS module.

We have first restored the Parrot AR to its default settings and conducted various flight sessions, each associated with image and video captures. The goal of our investigation was to recover as much data as possible, including the drone's path flight history and the media (images and videos) captured by the camera. We also aimed to explore ways of extracting the controller's ID to determine the ownership of the confiscated drone, as opposed to establishing pairing with the remote controller, reported previously in (Horsman, 2016). This is a relevant research objective given that the controller might not be available for the forensic investigators. We also aim to shed lights on some hurdles along the path of the drone's digital forensic investigation and showcase how to circumvent them.

Data Acquisition Phase

For the purpose of data acquisition, we have explored four access methods: Wireless connection via FTP or Telnet and direct connection via USB port or serial (UART) port connections.

Connecting to the Parrot AR and Acquiring Data Using a Wireless Connection

When powered up, the Parrot AR automatically boots up and becomes ready for use within seconds. It checks the motors and set up an unencrypted Wi-Fi hotspot named ardrone2_ followed by a 6-digits random number. In our case, the Wi-Fi hotspot is named ardrone2_011053. The Parrot uses Wi-Fi protocol to pair with its controller. By default, the connection is not password-protected.

After connecting to the Wi-Fi hotspot, a port scan using the *Nmap* tool on the drones IP has been performed as illustrated in Figure 4. As may be seen, the Parrot AR maintains an IP address of 192.168.1.1. The address 192.168.1.2 is the IP address of the investigation workstation (Kali Linux).

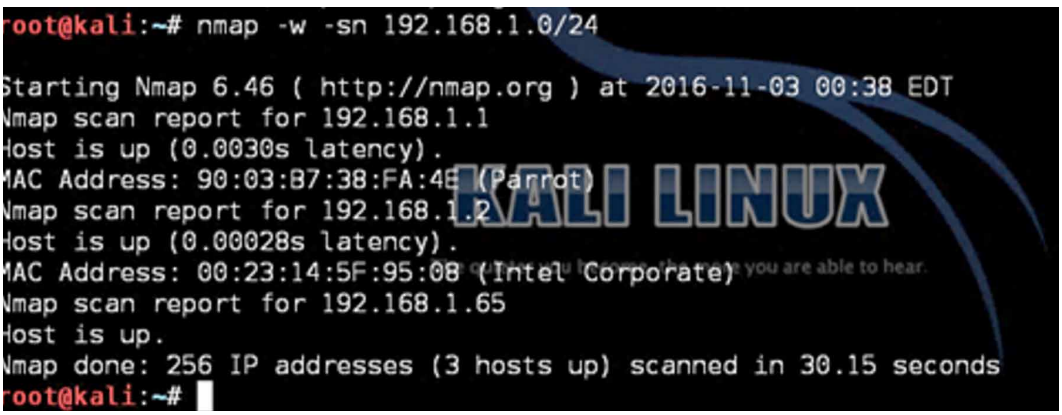
At this stage, the investigator has two options to access the content of the drone, namely a connection via a Telnet or via an FTP session, as shown in Figure 5.

Telnet Access

A Telnet session initiated to 192.168.1.1 connects directly to the Parrot AR and leads to a root shell. The root account is not password-protected which gives direct access to the entire Operating System and system files as shown in Figure 6. Using the "*netstat*" command, we were able to display

Figure 3. Flight recorder of the Parrot AR drone 2.0

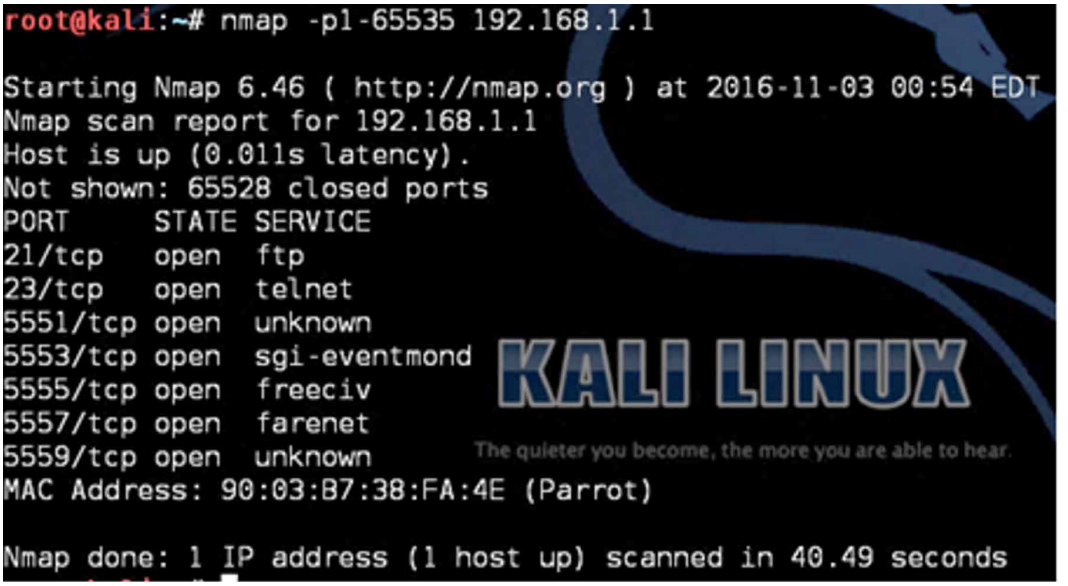
Figure 4. Port scan using Nmap



information about the state of the available network connections, which provides additional insights into other available ports on the Parrot AR. Table 1 provides a brief description of the main services offered by each defined port on the Parrot AR.

Once a Telnet session is established, issuing the *fdisk-l* command reveals the partition /dev/sda mounted, approximately 4 GB in size. Issuing the "*dd*" command on this partition, we were able to copy the content of the 4GB partition into an external USB device connected to the USB port of the flash memory (/dev/sdb). By doing so, we were able to access the full content of the "/data/video/usb" folder, which contains the media files.

Figure 5. Open ports on the Parrot AR Drone



FTP Access

As illustrated in Figure 7, the connection to the FTP service is not password protected, allowing anonymous ftp access to the /data/video/ subdirectory. Additionally, as illustrated in Figure 8, we were able to modify the file /etc/inetd.conf that defines the FTP daemon instances to authorize access to all directories that are available when connecting directly to the Parrot AR file system. Recall that the /etc/inetd.conf file is the default configuration file for the inetd daemon. This file enables to specify the daemons to start by default and supply the arguments that correspond to the desired style of functioning for each daemon. In our case, this was achieved by adding a master FTP daemon (21 stream tcp nowait root ftpd ftpd –w /) instance. Through this workaround, it was possible to access the system files and onboard resident data from an FTP connection. This is a new finding compared to the previous work reported by Horsman (2016), whereby FTP connection was reported to only provide access to media files.

Connecting to the Parrot AR and Acquiring Data Using a Direct Connection

In some cases, establishing a wireless connection to the Parrot AR may not be possible. In this situation, direct access is needed to retrieve some evidential information. This can be accomplished through a direct USB connection or via a serial connection, as further described below.

Accessing the Parrot AR and Acquiring Data Using a USB Connection

We connected directly to the Parrot AR via its USB port; the USB thumb drive is auto-mounted to /data/video/usb/ as shown in Figure 9.

This method allows direct access to the connected USB device which contains the Parrot AR Media folder. This Media folder contains pictures and videos stored on the Parrot's internal storage. Unfortunately, USB connection does not allow direct access to the physical disk for forensic imaging purposes. To circumvent this limitation, we explored other direct connection methods that would enable us to conduct forensic imaging and collect further forensic evidences.

Figure 6. List of system files of the Parrot using Telnet

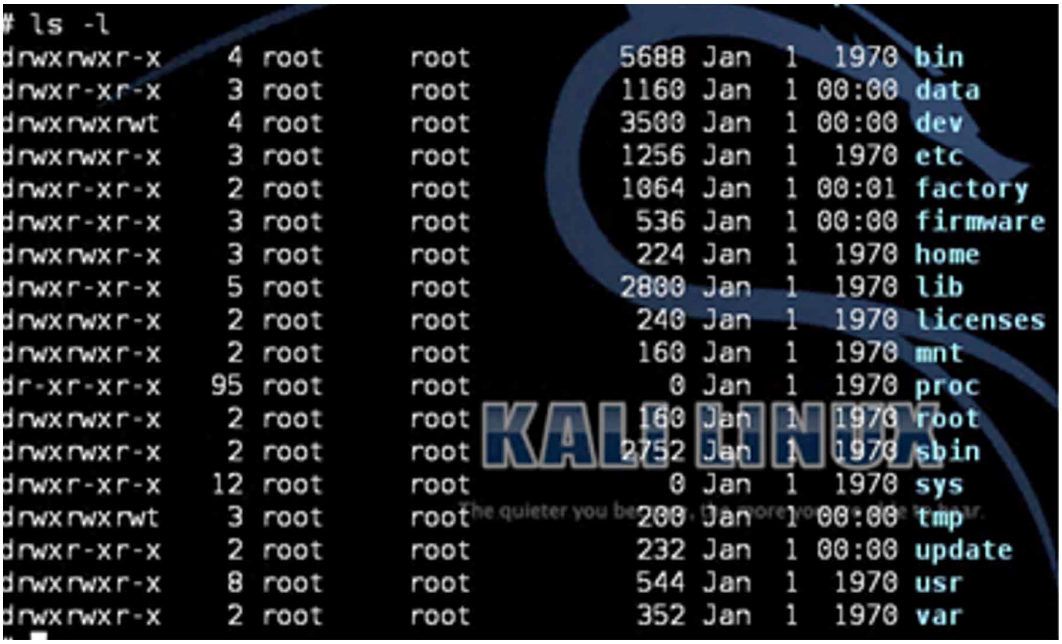


Table 1. Parrot AR port descriptions

Port	Service
21 (TCP)	*FTP* Server
23 (TCP)	*Telnet* Server
67 (UDP)	*DHCP* server to assign IP addresses to connected devices and communicate with dhcpv4 clients
5551 (TCP)	*FTP* access to retrieve drone's version and update firmware
5552	Authentication port
5553 (TCP)	*VIDEO* port: Used to transmit H264-720p frames when the application is recording
5554 (UDP)	*NAVDATA* port: Used to send navigation (telemetry) data to clients
5555(TCP)	*VIDEO* port: Used to send live video streams
5556 (TCP) (UDP)	*AT*-port: Used to send AT control commands to the drone
5557(TCP)	*RAW* capture port
5559 (TCP)	C*ONTROL* port: used to transfer critical configuration data

Accessing the Parrot AR and Acquiring Data Using Serial Console Connection

Using the experimental setup depicted in Figure 10, we were able to establish a serial console connection to the Parrot AR by using a CP210 USB-to-TTL converter and some additional wires.

Compared to a direct USB connection, the serial connection has the advantage of enabling the forensic investigator to gain access not only to the media files but also to the UAV's system files and onboard data. In fact, using a text-based serial port communications program (e.g., Tera Term), we were able to connect to the serial port of the Parrot AR and access its system files, as shown in Figure 11.

Figure 7. FTP connection to the Parrot

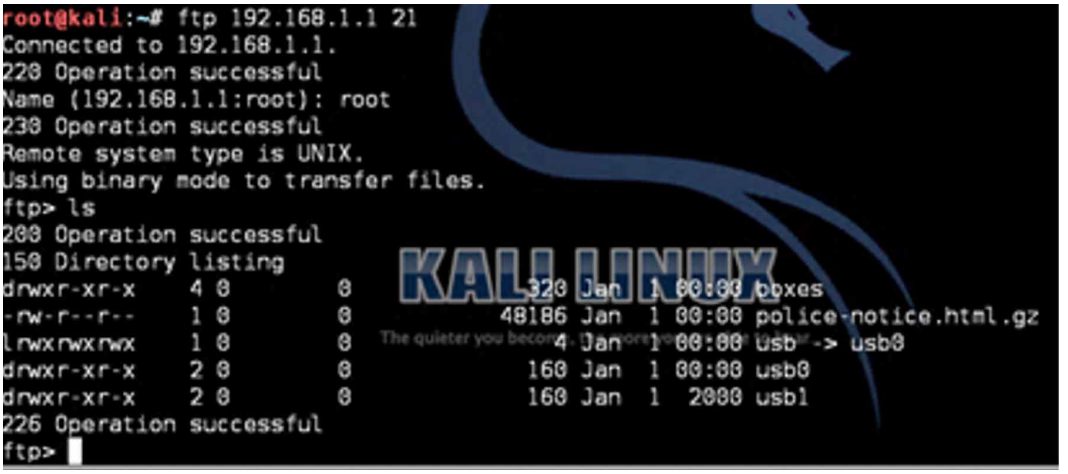


Figure 8. Content of '/etc/inet.conf' folder

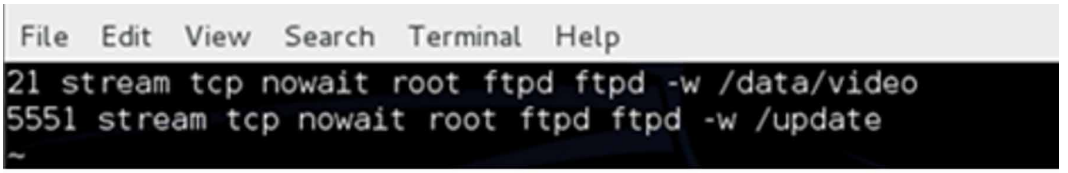


Figure 9. Structure of '/data/video' folder

The Analysis Phase

The various activities performed during the acquisition phase have enabled the collection of significant forensic data. These latter require deeper analysis in order to explore its usefulness as forensic evidence in a court of law.

Figure 10. USB to TTL connector using CP210 Bridge

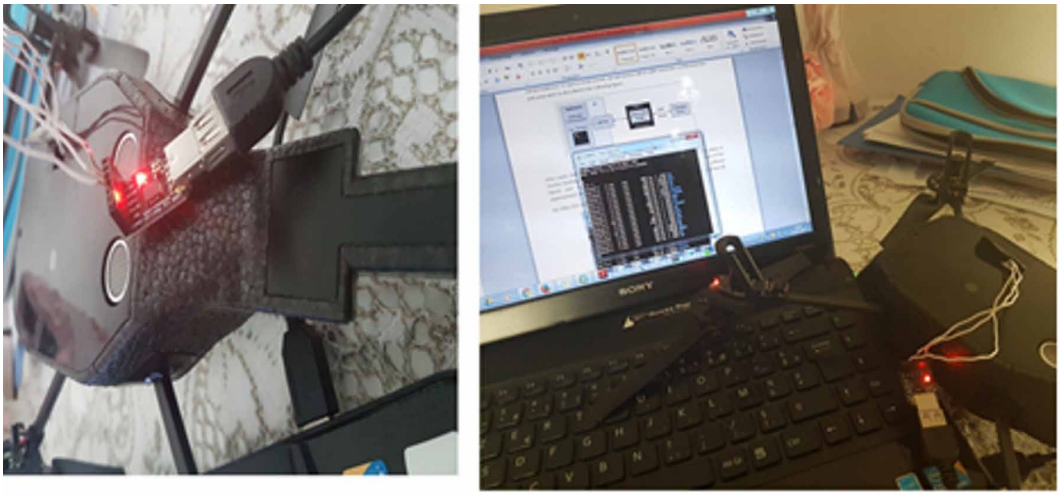
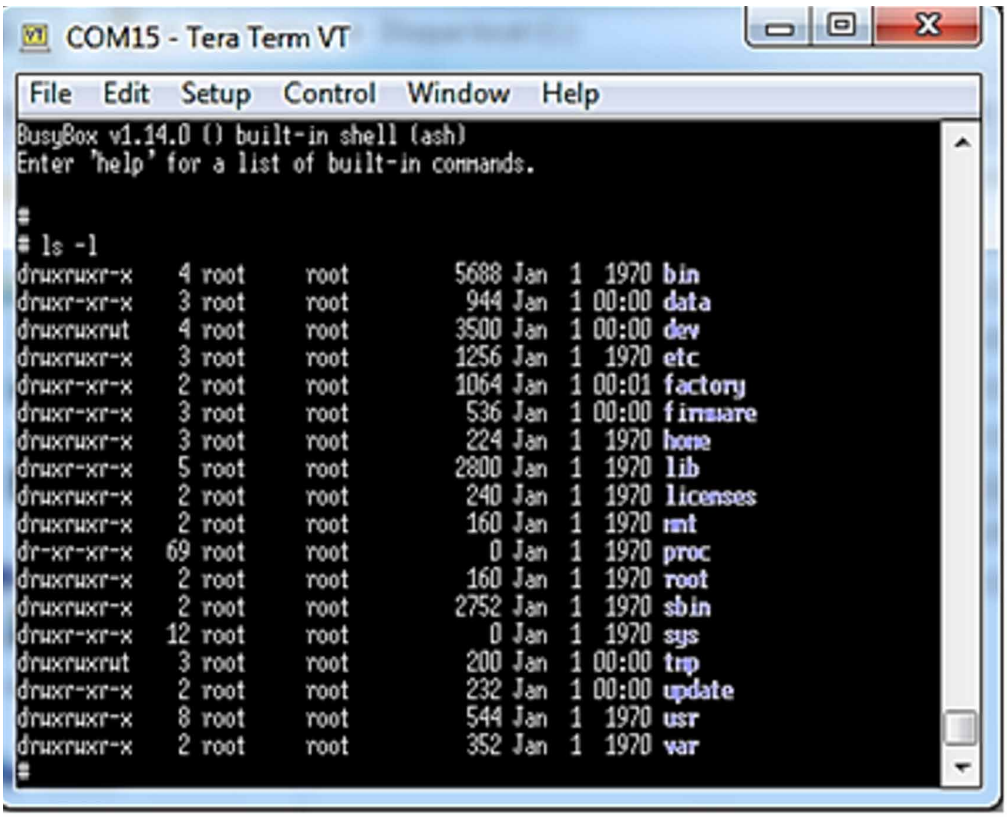


Figure 11. Accessing the Parrot AR system files



Establishing Flight Path Data

Among the main objectives of a drone forensic analysis is the extraction of its flight path history which allows the investigator to reconstruct the drone flight path and prove whether or not it was flying over a restricted area or no-fly zone.

As illustrated in Figure 12, the flight path history is stored under the "/data/video/" folder. More precisely, each time a flight session is established with the Parrot AR, a *userbox* file is created under the corresponding flight subdirectory. A *userbox* file is a binary file that has the following structure: /data/video/boxes/flight_YYYYMMDD_hhmmss/userbox_<timestamp> where <timestamp> represents the time since the Drone AR booted. This file (shown in Figure 13) contains both configuration details (e.g., firmware version, serial number, total flight time, flight settings) as well as navigation data (e.g., drone status, attitude, speed, sensor data, battery level, GPS details).

It is worth mentioning that for each flight session, the flight path data can be recovered from the mobile controller running (in our case) the AR.FreeFlight application, as long as the app does not connect to and upload this flight data onto the "AR Academy". In this case, for each flight session, the userbox file will also be stored in the subfolder flight_yyyymmdd_hhmmss under the Documents folder of AR. FreeFlight app. Each folder's naming convention reflects the date and time of the flight. To gain meaningful insights into the content of the userbox file, we used Darklo's Ruby script that takes a userbox file produced by Parrot AR and outputs a GPX file that can be opened by Google Earth application. A GPX file is an open GPS exchange format that is an XML schema designed as a common GPS data format for software applications. It can be used to describe GPS waypoints, tracks and routes.

In our experimental study, we carried out some sample flights as illustrated in Figure 14.

In addition, as highlighted in Figure 15, we were able to exfiltrate waypoints information for the flight path.

The content of the GPX file, shown in Figure 16, reveals useful forensic evidences which include:

- Name of the flight
- Track Segment which holds a list of Track points that are logically connected in order to represent a single GPS track: the path flight
- Latitude and longitude for the Parrot AR home point
- Flight-time
- Parrot AR's elevation

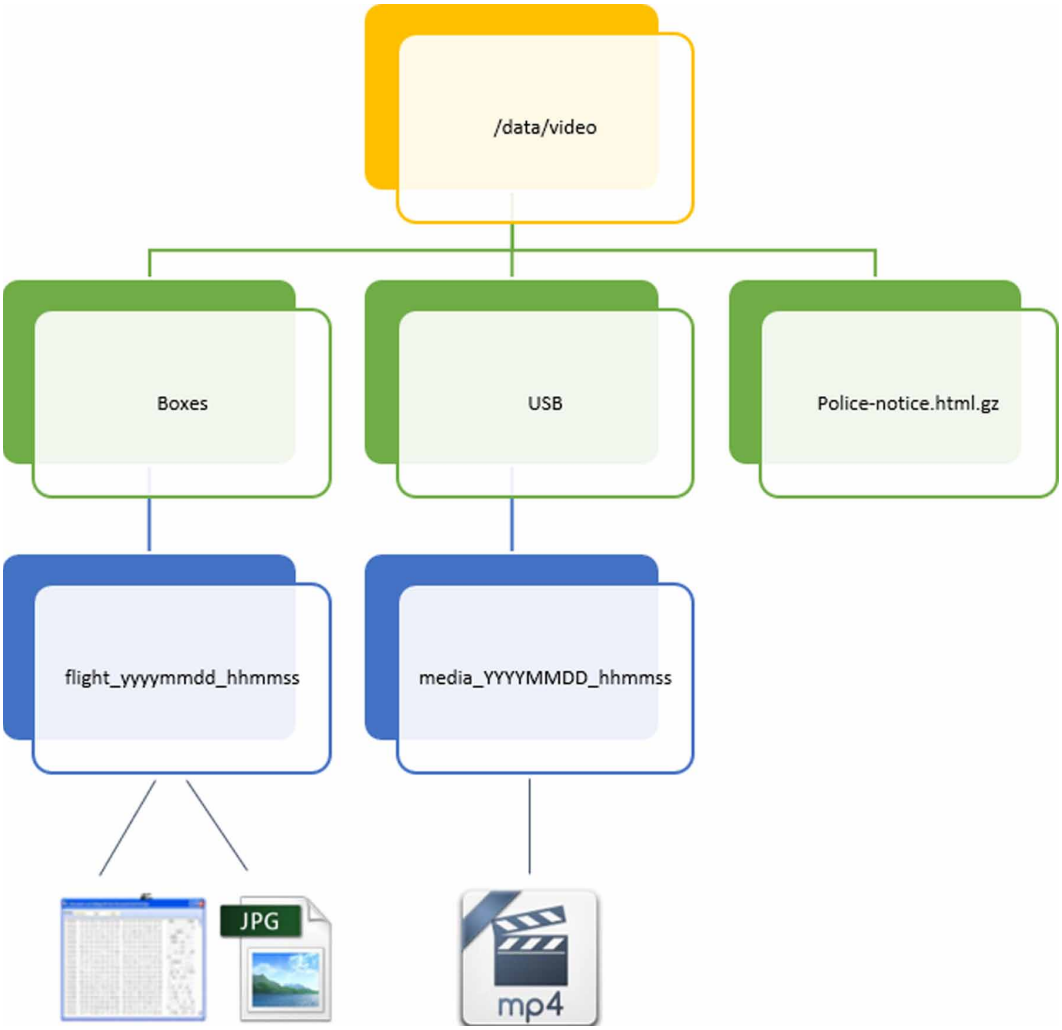
Accessing the Parrot AR Media Files

When the Parrot AR takes pictures, it saves them as JPEG images in its internal flash memory, named: /data/video/boxes/tmp_flight_YYYYMMDD_hhmmss/picture_YYMMDD_hhmmss.jpg, as previously illustrated in Figure 12. The flight directory is then downloaded via FTP on the Academy folder.

The flight recorder of the Parrot AR stores flight videos in its external flash memory as MP4 files (Figure 12) named /data/video/usb/media_YYYYMMDD_hhmmss /video_YYMMDD_hhmmss.mp4. These video files can also be retrieved from the control device. We investigated the files created for significant Exchangeable Image File format (EXIF) data and Time stamps. Given the fact that the Parrot AR is able to obtain a GPS lock, the camera will store latitude and longitude coordinates. On the other hand, if the drone is unable to lock to the GPS signal, the EXIF data does not contain GPS attributes.

In our case, we used the Exiftool utility to retrieve the EXIF data as illustrated in Figure 17.

Figure 12. Structure of "/data/video/" folder

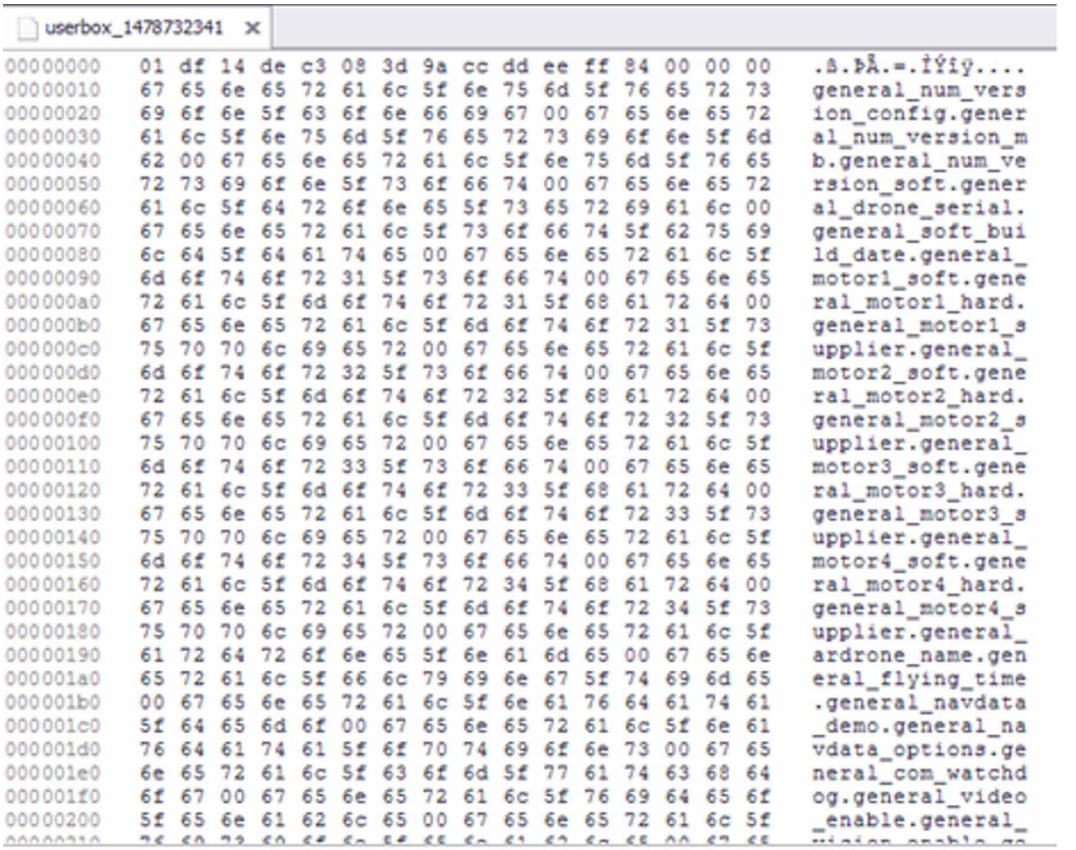


Identifying the Controller's ID and Establishing Ownership

Identifying the owner of a confiscated UAV based on information extracted solely from the drone was found to be an unviable task. Earlier research (Horsman, 2016) reported that searches within the Parrot Bebop UAV memory partition and operating system partitions did not reveal any information about the controller's ID (e.g., MAC address, serial number, IMEI number, MSISD number). However, when both the UAV and its controller are seized, it was possible to match the UAV Serial Numbers (SNs) found on both the UAV and its controller's handset to establish pairing between them and prove ownership (Horsman, 2016). In the case of the DJI Phantom III drone, Clark et.al (2017) demonstrated that when both the drone and the controlling mobile device are seized, it was possible to correlate extracted data and hence link the user to a specific device on the basis of the extracted metadata.

In our case, the pairing connection was easy to establish as the SN of the Parrot AR is readily accessible from the /factory/serial.txt file or the SN could be found on the body of the Parrot AR as shown in Figure 18.

Figure 13. Userbox file content


userbox_1478732341

```
00000000   01 df 14 de c3 08 3d 9a cc dd ee ff 84 00 00 00   .ß.ÞÃ.=.ÌÝîÿ....
00000010   67 65 6e 65 72 61 6c 5f 6e 75 6d 5f 76 65 72 73   general_num_vers
00000020   69 6f 6e 5f 63 6f 6e 66 69 67 00 67 65 6e 65 72   ion_config.gener
00000030   61 6c 5f 6e 75 6d 5f 76 65 72 73 69 6f 6e 5f 6d   al_num_version_m
00000040   62 00 67 65 6e 65 72 61 6c 5f 6e 75 6d 5f 76 65   b.general_num_ve
00000050   72 73 69 6f 6e 5f 73 6f 66 74 00 67 65 6e 65 72   rsion_soft.gener
00000060   61 6c 5f 64 72 6f 6e 65 5f 73 65 72 69 61 6c 00   al_drone_serial.
00000070   67 65 6e 65 72 61 6c 5f 73 6f 66 74 5f 62 75 69   general_soft_bui
00000080   6c 64 5f 64 61 74 65 00 67 65 6e 65 72 61 6c 5f   ld_date.general_
00000090   6d 6f 74 6f 72 31 5f 73 6f 66 74 00 67 65 6e 65   motor1_soft.gene
000000a0   72 61 6c 5f 6d 6f 74 6f 72 31 5f 68 61 72 64 00   ral_motor1_hard.
000000b0   67 65 6e 65 72 61 6c 5f 6d 6f 74 6f 72 31 5f 73   general_motor1_s
000000c0   75 70 70 6c 69 65 72 00 67 65 6e 65 72 61 6c 5f   upplier.general_
000000d0   6d 6f 74 6f 72 32 5f 73 6f 66 74 00 67 65 6e 65   motor2_soft.gene
000000e0   72 61 6c 5f 6d 6f 74 6f 72 32 5f 68 61 72 64 00   ral_motor2_hard.
000000f0   67 65 6e 65 72 61 6c 5f 6d 6f 74 6f 72 32 5f 73   general_motor2_s
00000100   75 70 70 6c 69 65 72 00 67 65 6e 65 72 61 6c 5f   upplier.general_
00000110   6d 6f 74 6f 72 33 5f 73 6f 66 74 00 67 65 6e 65   motor3_soft.gene
00000120   72 61 6c 5f 6d 6f 74 6f 72 33 5f 68 61 72 64 00   ral_motor3_hard.
00000130   67 65 6e 65 72 61 6c 5f 6d 6f 74 6f 72 33 5f 73   general_motor3_s
00000140   75 70 70 6c 69 65 72 00 67 65 6e 65 72 61 6c 5f   upplier.general_
00000150   6d 6f 74 6f 72 34 5f 73 6f 66 74 00 67 65 6e 65   motor4_soft.gene
00000160   72 61 6c 5f 6d 6f 74 6f 72 34 5f 68 61 72 64 00   ral_motor4_hard.
00000170   67 65 6e 65 72 61 6c 5f 6d 6f 74 6f 72 34 5f 73   general_motor4_s
00000180   75 70 70 6c 69 65 72 00 67 65 6e 65 72 61 6c 5f   upplier.general_
00000190   61 72 64 72 6f 6e 65 5f 6e 61 6d 65 00 67 65 6e   ardrone_name.gen
000001a0   65 72 61 6c 5f 66 6c 79 69 6e 67 5f 74 69 6d 65   eral_flying_time
000001b0   00 67 65 6e 65 72 61 6c 5f 6e 61 76 64 61 74 61   .general_navdata
000001c0   5f 64 65 6d 6f 00 67 65 6e 65 72 61 6c 5f 6e 61   _demo.general_na
000001d0   76 64 61 74 61 5f 6f 70 74 69 6f 6e 73 00 67 65   vdata_options.ge
000001e0   6e 65 72 61 6c 5f 63 6f 6d 5f 77 61 74 63 68 64   neral_com_watchd
000001f0   6f 67 00 67 65 6e 65 72 61 6c 5f 76 69 64 65 6f   og.general_video
00000200   5f 65 6e 61 62 6c 65 00 67 65 6e 65 72 61 6c 5f   _enable.general_
```

The Serial Number information also appears on the smartphone (e.g., under the /storage/emulated/0/Android/data/com.parrot.freelight/cache directory). These two pieces of information can be used to establish pairing of the UAV with its controller.

We have explored other means to establish ownership. As illustrated in Figure 19, all identified application settings are stored in /data/custom.config/ folder, under subfolders applis, profiles and sessions, written as follows: config.<id>.ini. The last element of the config.ini file displays the profile description. This description is set as [“.”.”build manufacturer (model)”:Android ID].

In Figure 19, the profile description shows [.Samsung_SM_G935F:ee8840cd20342521], where:

- Samsung_SM_G935F specifies the brand name and version of the controller.
- ee8840cd20342521 is the Android ID which is a unique device identification number. This is a random alphanumeric identification code string that is generated during the first boot of the device. It is used to uniquely identify users, for the purpose of market downloads of gaming applications.

The Android ID, which is a unique ID to each device, can be used by legal authorities to identify the mobile device and eventually its owner. This finding adds to the earlier contribution reported by Horsman (2016) by suggesting that it would be possible to retrieve information about the controller’s ID and eventually prove ownership of a captured Parrot AR drone based on its resident information.

Figure 14. Flight path carried on the Parrot AR

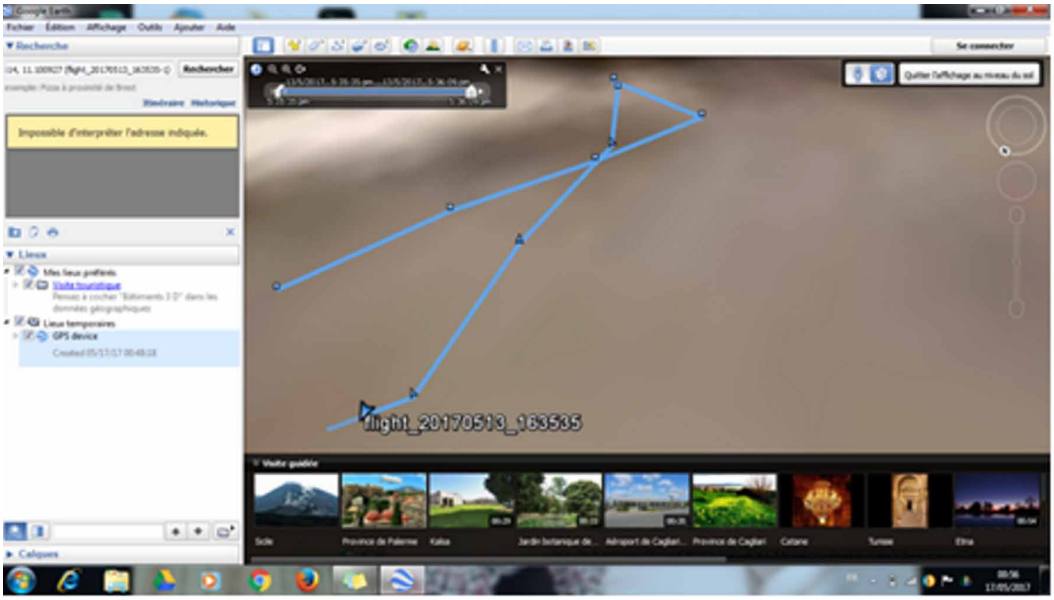
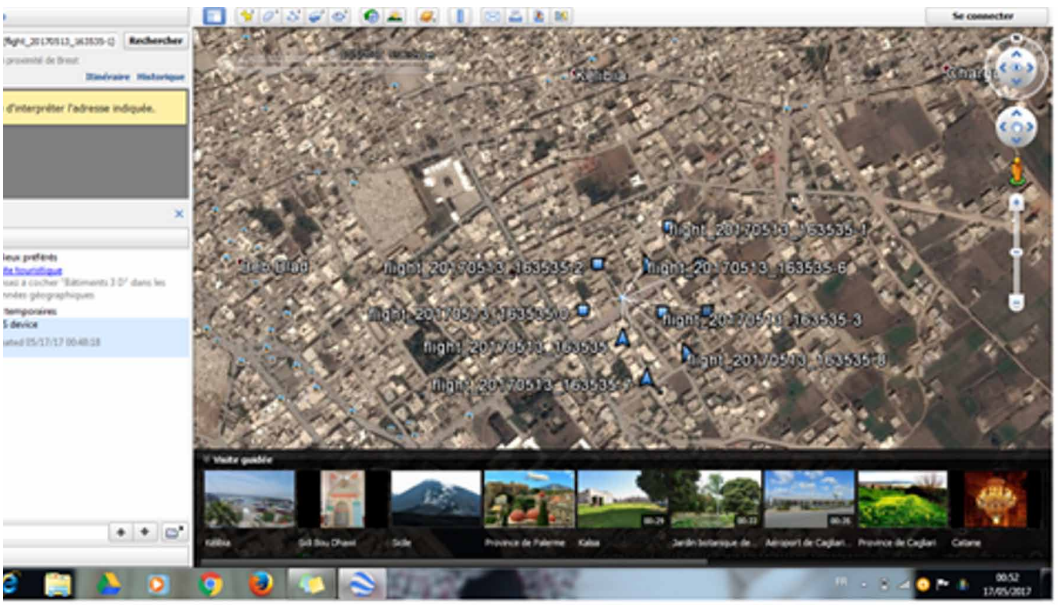


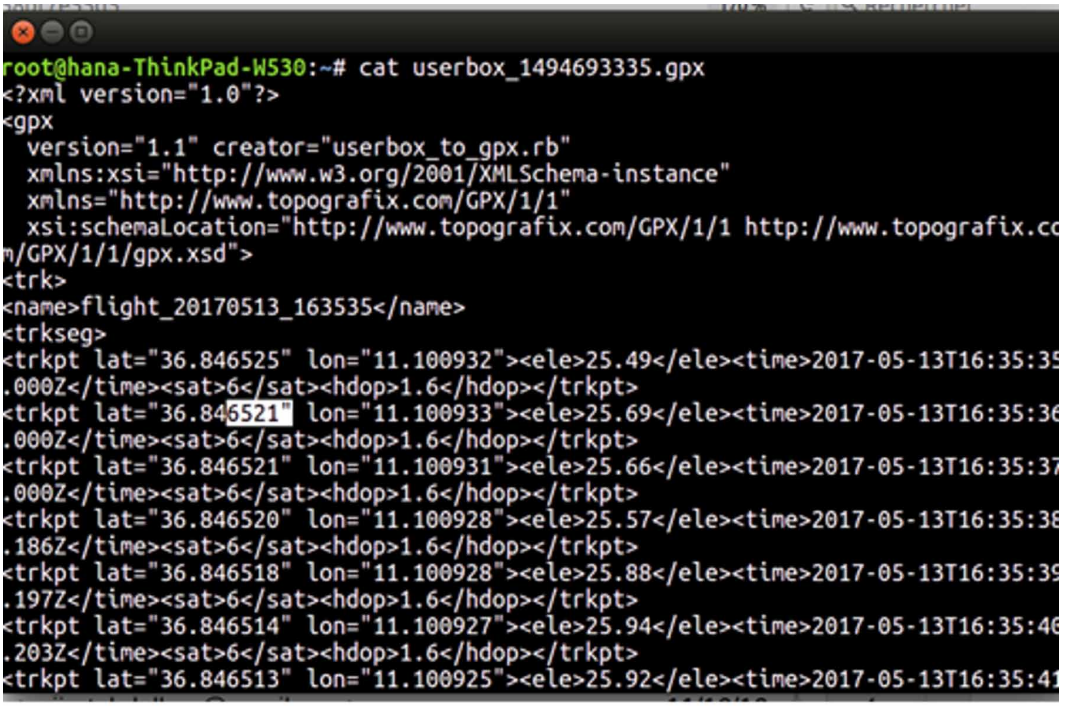
Figure 15. Waypoints on Google Earth application



CONCLUSION

This study highlights key challenges in drone forensics and presents the results of a forensic analysis performed on a Parrot AR drone 2.0. Our analysis adds new insights to the existing body of knowledge on drone forensics. They include the ability to access the file system from FTP or serial connections as well as the retrieval of the controller's Android ID that can be used to establish ownership. While this

Figure 16. The content of userbox.gpx file



contribution asserts the commonalities between drone forensics and other computing device forensics, it also highlights some peculiarities and unique challenges of performing forensic investigation on drones. It is worth mentioning that this study is focused on Parrot AR drone 2.0. This work can be extended to carry further forensic analysis on the Parrot AR and its controller, as well as on other UAVs in order to infer analogies and dissimilarities. Moreover, the JTAG and chip-off analysis could be explored to extract more evidence from potential damaged drones.

ACKNOWLEDGMENT

This research was supported by Zayed University Research Incentive Fund (RIF) grant #R16096 and R16083.

Figure 17. EXIF data retrieved from a picture taken by the Parrot AR

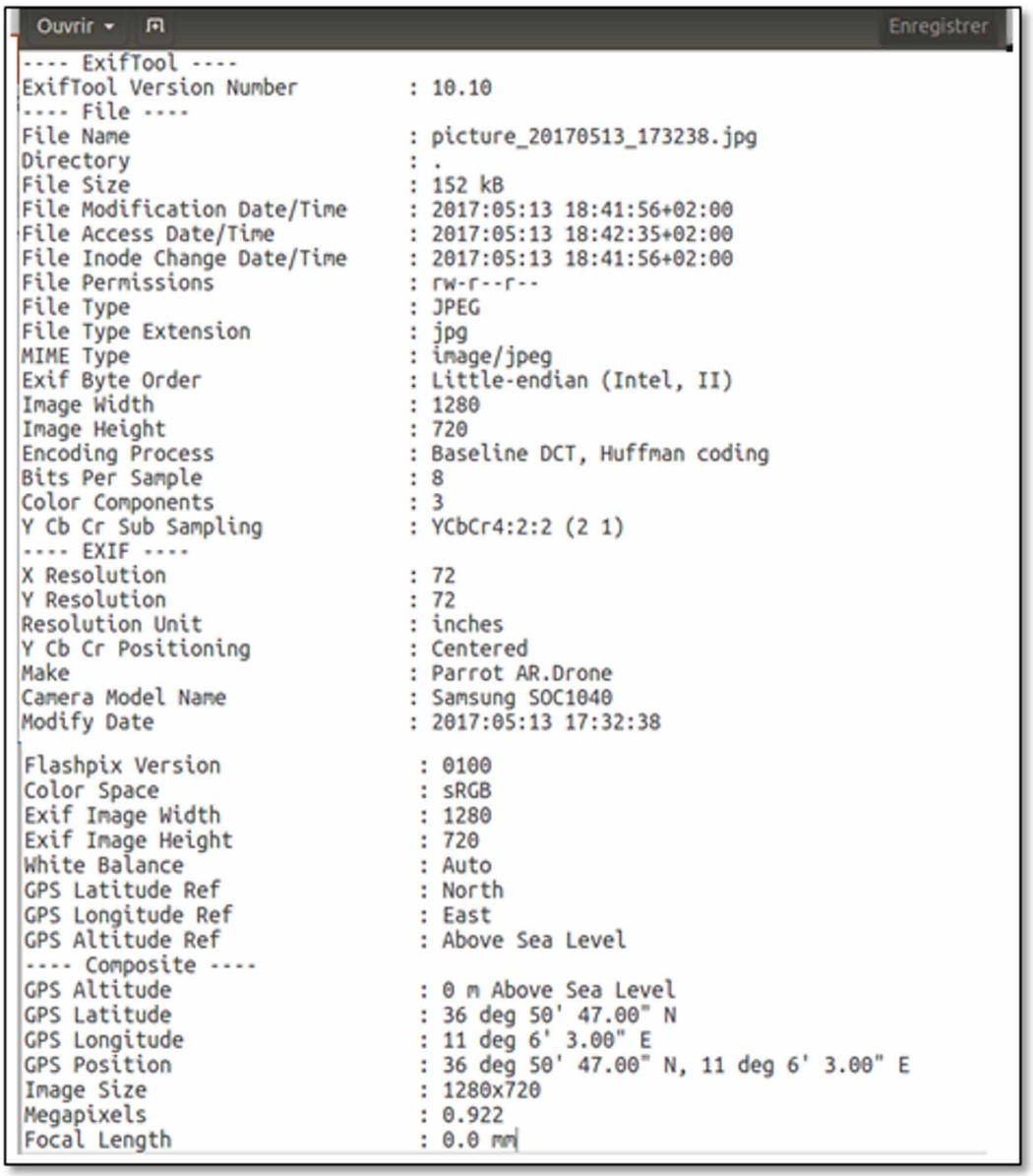
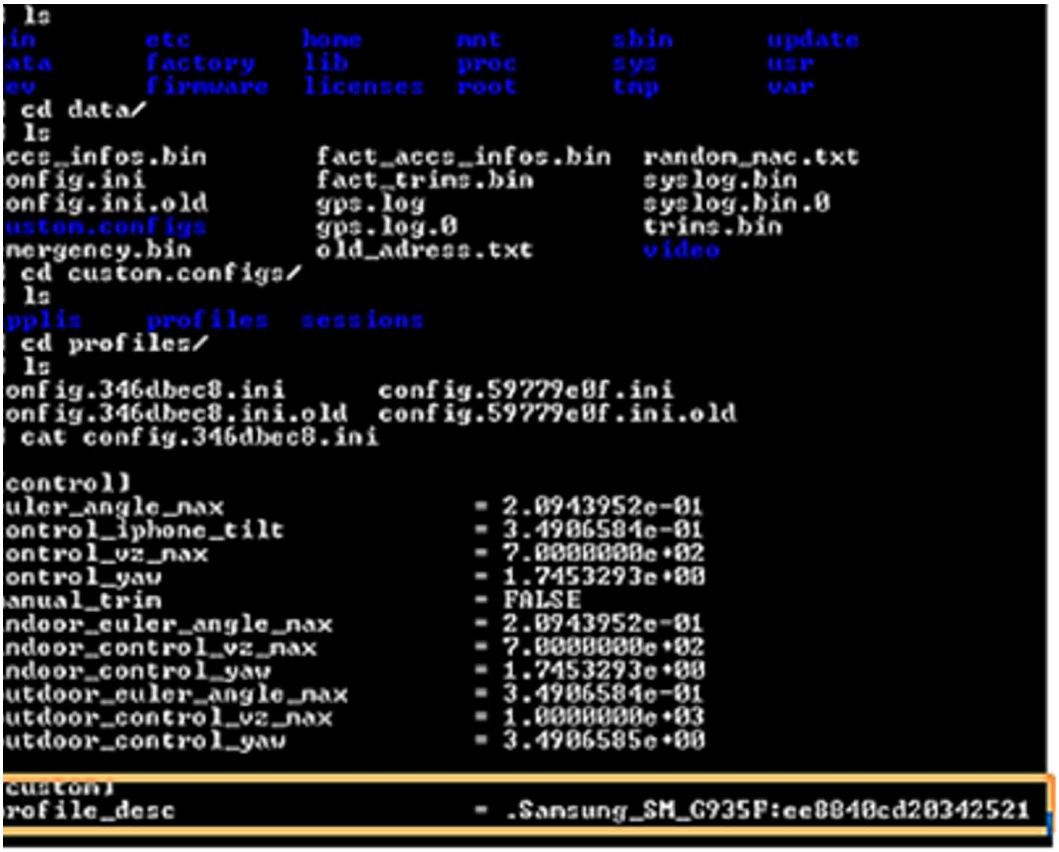


Figure 18. The serial number of the Parrot AR

Figure 19. Description of the content of the repository /data



REFERENCES

Camhi, J. (2016). Here are the technologies that are making drones safer and accelerating adoption. *Business Insider*. Retrieved from http://www.businessinsider.fr/us/the-drones-report-market-forecasts-key-players-and-use-cases-and-regulatory-barriers-to-the-proliferation-of-drones-2016-3/

Clark, D. R., Meffert, C., Baggili, I., & Breitinger, F. (2017). DROP (Drone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. In *Proceedings of the Seventeenth Annual DFRWS*, Austin, TX, August 6-9, pp S3-S14. doi:10.1016/j.diin.2017.06.013

Elands, P. J. M., de Kraker, J. K., Laarakkers, J., Olk, J. G. E., & Schonagen, J. J. (2016). Technical aspects concerning the safe and secure use of drones. In *Proceedings of TNO 2015.* Retrieved from http://publications.tno.nl/publication/34620203/zTAOSq/TNO-2015-R11721.pdf

Hasan, M., Iqbal, F., Hung, P. C. K., Fung, B. C. M., & Rafferty, L. (2018). A security study for smart metering systems. *International Journal of Urban and Civil Engineering*, *5*(1), 1–11.

Hoog, A. (2011). *Android forensics: Investigation, analysis and mobile security for Google Android* (3rd ed.). MA: Elsevier. doi:10.1016/B978-1-59749-651-3.10001-9

Horsman, G. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation*, *16*, 1–11. doi:10.1016/j.diin.2015.11.002

Hung, P. C. K., Kanev, K., Iqbal, F., Mettrick, D., Rafferty, L., Pan, G. P., . . . Fung, B. C. M. (2016). A Study of children facial recognition for privacy in smart TV. In *Proceedings of the International Symposium Computational Modeling of Objects Represented in Images* (pp. 229-240). Academic Press.

Hyde,W. (2014). Will the future of digital forensics and law enforcement investigation strategies need to adapt to malicious hardware devices? *Fifth annual Stevenson University Forensics Journal*, 5, 59-63.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST*. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Khanji, S., Jabir, R., Iqbal, F., & Marrington, A. (2016). Forensic analysis of Xbox One and PlayStation 4 gaming consoles. In *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)* (pp. 1-6). IEEE. doi:10.1109/WIFS.2016.7823917

Kovar, D. (2015). *Drone forensics – An overview*. Retrieved from https://integriography.wordpress.com/2015/03/15/drone-forensics-an-overview/

Paganini, P. (2014). Wireless aerial surveillance platform: the DIY spy drone. *Security Affairs*, Retrieved from http://securityaffairs.co/wordpress/31190/hacking/wireless-aerial-surveillance-platformdiy-spy-drone.html

Peacock, M., & Johnston, M. N. (2013). Towards detection and control of civilian unmanned aerial vehicles, In *Proceedings of the 14th Australian Information Warfare Conference*, Edith Cowan University, Perth, Western Australia, December 2-4 (pp. 9-15). Academic Press.

Pickard, A. (2016, April 8). Charges dropped in Oklahoma prison alleged drone smuggling attempt, pending lab tests. *Tulsa World*. Retrieved from http://www.tulsaworld.com/news/courts/charges-dropped-in-oklahoma-prison-alleged-drone-smuggling-attempt-pending/article_7c17cca3-b0bf-53cd-95e9-f3bf5e227441.html

Rafferty, L., Hung, P. C. K., Fantinato, M., Marques Peres, S., Iqbal, F., Kuo, S. Y., & Huang, S. Y. (2017). Towards a privacy rule conceptual model for smart toys. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 1226-1235). Academic Press. doi:10.24251/HICSS.2017.146

Ravich, T. M. (2015). Commercial drones and the Phantom menace. *Journal of International Media and Entertainment Law*, *5*(2), 175–215.

Singh, A. (2015). Drone forensics: An unrevealed dome. *Data Forensics*. Retrieved from http://www.dataforensics.org/drone-forensics/

Sivakumaran, P. (2014). Analyzing application data Security on Android devices. Royal Holloway, University of London. Retrieved from https://www.ma.rhul.ac.uk/static/techrep/2014/RHUL-MA-2014-12.pdf

Thiobane, F. (2016). *Cybersecurity and drones, MSc Capstone project*. UTICA College.

Yunus, Y., Roslan, I., & Zainuddin, H. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology*, *3*(3), 17–31. doi:10.5121/ijcsit.2011.3302

Hana Bouafif is a professor at Esprit, Tunisia since September 2010. Since December 2012, she has been coordinator of the Networks, Infrastructure and Data Security (NIDS) specialty. She obtained her master's degree in computer networks research from the Higher School of Communication of Tunis (Supcom, Tunisia) in June 2012. Her research interests include information security, social networking and digital forensics. She has been successful in publishing her work in peer reviewed conferences and journals.

Faouzi Kamoun is a professor at ESPRIT School of Engineering, Tunisia. He holds a PhD in Electrical Engineering from Concordia University and an MBA in Management from McGill University, Canada. Prior to joining ESPRIT in 2015, he held various academic and administrative positions at Zayed University and at the University of Dubai, UAE. His research interests include technology management, security, applied research on IoT/smart-cities, and social innovation.

Farkhund Iqbal is an Associate Professor and Director, Advanced Cyber Forensics Research Laboratory in the College of Technological Innovation, Zayed University, United Arab Emirates. He holds a Master (2005) and a Ph.D. degree (2011) from Concordia University, Canada. He is using machine learning and Big Data techniques for problem solving in healthcare, cybersecurity and cybercrime investigation in smart and safe city domain. He has published more than 80 papers in high ranked journals and conferences. He is an affiliate professor in school of information studies, McGill university, Canada and Adjunct professor in Adjunct Professor, Faculty of Business and Information Technology Ontario Tech University (OTU), Canada, Canada. He is the recipient of several prestigious awards and research grants. He has served as a chair and TPC member of several IEEE/ACM conferences, guest editor of special issues and reviewer of high rank journals.