GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

UNMANNED AERIAL VEHICLE (UAV) – A NEW CHALLENGE FOR ELECTRONIC FORENSICS INVESTIGATION FOR THEIR REPOSITORIES

P N RAMAKRISHNAN

ASSISTANT DIRECTOR & SCIENTIST-C (PHYSICS)
CENTRAL FORENSIC SCIENCE LABORATORY
DIRECTORATE OF FORENSIC SCIENCE SERVICES
MINISTRY OF HOME AFFAIRS, GOVT. OF INDIA
RAMANTHAPUR, AMBERPET, HYDERABAD
TELANGANA STATE
09440697407, Fax:040-27039281
pnrkrishnan.cfsl@gov.in; pnrkrishna@rediffmail.com

Abstract

Since past ten years there has been drastic increase in the utility of 'Unmanned Aerial Vehicle (UAV)' which are commonly called as "UAV's" in the field of aerial videography, photography, traffic monitoring, riot monitoring and other aerial visualization and recording. Also, in recent, e-commerce companies have experimented of dropping the deliveries at the destination through the UAV's. In recent past it was observed that these UAV's have been found paving its way into anti-social elements, anti-national activities, terrorism both internal and external like utilizing for dropping of drugs and firearms for their secure trafficking. The crimes like disruption of air traffic control stations jamming, aerial photography/videography of defence installations, troop movements tracking, videography of vital power-stations, dams etc. have come to light to the investigation and intelligence agencies. In India, the recent terrorist activities recently, wherein the UAV's have been supposed to be used by the anti-state organizations. As on date, standard method of extraction or repository related dated available in the Unmanned aerial vehicles are not available. Once, these UAV's are captured from S.O.C., the dearth of information and data in their repositories like launch details, landing details, logs of activities of operation, waypoints, GPS location data, flight track data, cloud data information pertaining to UAV's and other video/still imageries etc. are highly valuable for the investigation and in Court of Law. This paper envisages the use of open source technologies and other computer forensic tools for the extraction of the valuable data from the repositories as well as the other relevant Operating Systems (OS) used in the UAV's and their peripherals like remote controller, Ground Control Station, Tablets, Smart phones or laptops or computers.

Keywords: *Electronic Forensics, Data retrieval, Repositories, UAV's.*

INTRODUCTION

The Unmanned Aerial Vehicles (UAV) which are commonly called as "DRONE" are hovered through remote control along with onboard Ground Control Station which are normally tablets, laptops, computers or even smart phones. The UAV's were designed for multipurpose utility as surveillance by law enforcement agencies, rescue team operation, e-commerce, aerial videography and photography, digital mapping by surveyors/land registration departments and other numerous applications

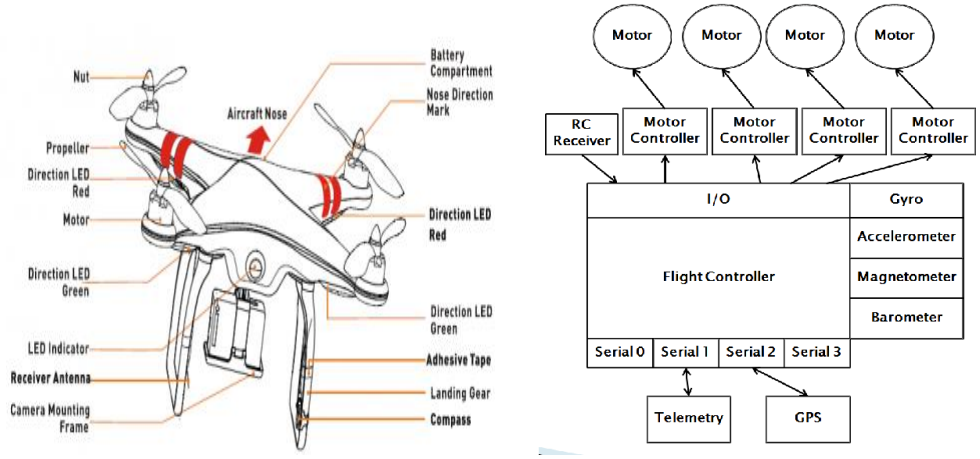
There are more than dozen commercially popular branded UAV's in the market which varies depending on their range of operation, the resolution right now upto 4K/HD quality and cost of the UAV's. Most popular UAV's are like Parrot, Phantom, SKyviper, Mavic, Rover, Typhoon etc.

The common UAV's flying ranges varies from 0.3 kilometers to 5 kilometers with flight speed varying from 16 meters per second to 20 meters per second. The remote controlled UAV's have the transmitter for operation with Radio Frequency (RF) of 2.4 GHz frequency band, however many other factors may be influenced during the flight. The good operation zone of any UAV's is governed by the communication made by transmitter and receiver of the UAV's which are namely in the shape of ellipsoid called Fresnel Zone.

UAV's are broadly consists of (i) Unmanned Aerial System (UAS), (ii) Ground Control Station (GCS) and (iii) the controller, which are required for flight control in a successfully maneuver by remotely controlling.

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

System Block Diagram



(Figure – 1 Parts of Drone and its schematic diagram – Courtesy BestDroneUnderHalfaPound.com & ICISET2016)

Recent incidents of UAV's being utilized for drug dropping, firearm dropping, airport UAV's chaos, spying, aerial photography/videography of vital installations by criminals, terrorists, anti-social and antinational organizations have been reported.

The complexity of repositories and identifying the artifacts from the UAV's is an upcoming and challenging area in the field of electronic forensics. Also, the literature survey showed that there is a wide potential scope for development and improvisation of the validated forensic software. As on date only certain Open Source tools and conventional trial and error is being implemented for recovery of forensic electronic data from the UAV's.

RECENT CASES OF UAVs

Many cases are being reported wherein UAVs/Drones are being utilized in the antinational and antisocial activities. Recently, in India the attack using the drone on a military sensitive area by the cross border terrorists have been in news. The seized drones were sent for the complete data analysis for obtaining valuable information for the state security purposes. There are also intelligence reports that these can be used for dropping bombs, supply of narcotics substance and other anti-national purposes.

Even the State Government like Government of Telangana has recently utilized the Drones for the supply of medicines and other medical article to the remote village health centres. Non touch by human interference during this COVID pandemic has seen the important in the e-commerce business for dropping of the items or articles procured to the customers so as to maintain the social distancing. For geological purpose, like 3-D mapping of hills, forest vegetation, fishing areas of cross border waters etc. It is also valuable during the natural calamities to judge the damage caused were the humans cannot go during such devastation areas and can be utilized in rescue operations. As Wild Life Act in India is now making news where prominent personalities were found misusing the wild life animals in the name of hunting and endangering the wild life in the nature. This UAVs surveillance and their tagging movement may improve for the ecological imbalances. The aerial photography by the UAVs/Drone have in important role during the large mass agitations and riot control activities by the Police and law enforcement agencies.

Drones or UAVs can be used by the Forensic Scientists during the complete videography of the Scene of Crime incidences as it is now mandatory by the Hon'ble Supreme Court of India. Such captured videos or photographs can be utilized in the Reconstruction of Scene of Crime and to prove in the Hon'ble Court of Law. During COVID pandemic, the law enforcement agencies have utilized the UAVs/Drones for identifying the netizens who were found not obeying the 'LOCK DOWN' rules. These photographs and videos were utilized as evidence as a part of Disaster Management Acts of India by various state and central governments.

UAV'S FORENSIC CHALLENGES

The literature and technical data of the UAV's showed that a common similarity could be seen in the UAV's and the modern smart phones. A wide range of data artifacts can be obtained from the different repositories which can be both covert and overt storage locations of the UAV's. The most commonly and that easily can be obtained with conventional electronic forensic software/hardware tools from the storage devise that can be found is in the form of Micro-SD cards or Flash Storage Devices.

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

It is a must as per the cardinal rules of electronic forensics that the principle of integrity of original data should be sustained. It is however, emphasized that a authentic and validated forensic extraction of data from the repositories of the UAV's could be more useful for maintaining the consistency of the data recovery.

2(a) **Repository Location of the UAV's**

Commonly found are like in the mobile devices, the UAV's also uses a medium for the storage of data which may be either Micro-SD card or Flash Memory Storage devices.

2(b) **Ground Control Station**

Normally a computer, laptop or tablet or even a modern smart phones are being utilized as Ground Control Unit. Like other conventional forensic analysis, a dearth of data which could be useful for the investigating agencies can be obtained.

2(c) **Various Artifacts retrieved from Repositories**

From the ground control unit media like laptops, computer, tablet or mobile phones the Operating System (OS) which is proprietary for a particular manufacturer of UAV's can be identified. This OS can be utilized for address protocol of UAV's, scripting environment, file system identification and type of system data logs etc.

The UAV's have the valuable information related to GPS, altitude of flying, the speed or velocity of the UAV's during their flight, the battery level of charging etc. These can be collected from both UAV's main unit or from GCU.

The Way Points assisted by the GPS can also be a valuable data s it can be linked to the data directly with the live Google maps for the region of travel by the UAV's also its map imagery data base. This will help to identify the area coordinates of a particular geographical area.

The log data from 'cache' of the repositories from the media of the UAV's have an important artifacts related to flight data. These data are pertaining to take-off and landing of the UAV's which are controlled via GCU and other commands given to the UAV's from ground.

Apart from these above data, the UAV's repository have the complete video and image data along with their thumbnails which could have been captured during its flight of operation.

2(d) **The File Systems of the UAV's**

The file system of UAV's form an important part of the forensic electronic investigation. Identification of the file system which can be simple 'txt' file and extends to the files like 'dat', 'exif-DCIM', XML file, Config.in, syslog, USBkey Writer, dji.pilot.log, cache files etc. are the base of the retrieval of all vital information contents of the UAV's. Each files are to be identified independently and making it into readable and reportable format makes the very essence of challenge to the electronic forensic scientist or investigators.

Some of the commonly utilized Open Source Software tools for UAV's forensic analysis are DROP (UAV's Open Source Parser), Exiftool, FTK toolkit, CelleBrite, Magnet AXIOM, Csv-View tool, Cloud forensic tool software, DatCon, DCode and Google Earth live etc. Single application cannot be restricted for the entire repository retrieval of data of the UAV's.

CONCLUSION

The technology of the UAV's would be refined in the days to come and the complexity of retrieval of data from the repositories of the UAV's would be more challenging for the experts. The forensic relevant artifacts and their recovery would be a potential area of interest for the future research also. With an effective validated development of the software for the UAV's can be well utilized in future UAV's based cyber attack analysis and investigation.

ACKNOWLEDGMENT

I thank my Director, Central Forensic Science Laboratory(CFSL), Hyderabad for his constant support and encouragement. I also thank my colleagues from the Digital Forensic Division, CFSL, Hyderabad who provided insight and expertise that greatly helped me to write this paper. I finally thank my colleagues of Physics Division, CFSL, Hyderabad for their continuous contribution during the literature survey for this paper.

REFERENCES

[1] DRONE Forensic Analysis using Open Source Tools, Journal of Digital Forensic Security & Law; Vol.13, No:1, Article-6.
[2] Open Source Forensic for a multiplatform UAV's System, ICFS &Cyber Law, Prague, 2017, 83-96.
[3] UAV(aka DRONES) Forensics/2015/Digital Forensic and Incident Response Summit.
[4] UAV-A preliminary analysis of forensic challenges, Digital Investigation (16(4)/p-1-11.
[5] Validation of Forensic Tools & Software; A quick guide for the Digital Forensic Examiner.
[6] Digital Forensic on a DJI Phantom mission, 2016.

[7] Gazette Notification of Government of India's "The Unmanned Aircraft System Rules, 2020 dated 2nd June 2020.
[8] Application of Drone in the Investigation and Management of Crime Scene, Volume 4, Issue-4, April, 2015, Global Journal for Research Analysis, ISSN No.:2277-8160.
[9] Research Challenge based opportunities in Drone Forensics Models, Journal-Electronics 2021, issue-10, 1519.
[10] An amateur drone surveillance system based on the cognitive Internet of Things, IEEE Communication Magazine, 2018, 56, 29-35.
[11] Detection, tracking and interdiction for amateur Drones, IEEE Communication Magazine, 2015, 56, 75-81.
[12] An approach to Unmanned Aerial System Forensic Frame Work, Pro-Quest, Capitol Technology University, Laurel, MD, USA, April, 2019.
[13] A Comprehensive micro-UAV Forensics frame work, Digital Investigation Journal, 2019, 30, 52-72.
[14] UAV Digital Forensic Investigation Frame work, Journal of navigation Science Engineering 2018, 14, 32-53.
[15] Drone Forensic Investigation: DJI Spark Drone as a case study, Journal - *Procedia* Computer Science /Science Direct, 159(2019), 1890-1899.