CERIAS

The Center for Education and Research in Information Assurance and Security

Drone Disrupted Denial of Service Attack (3DOS): Towards an Incident Response and Forensic Analysis of Remotely Piloted Aerial Systems (RPASs)

Fahad Salamh fsalamh@purdu.edu , Dr. Umit Karabiyik ukarabiy@purdue.edu , Dr. Marcus Rogers rogersmk@purdue.edu

Abstract

According to the Federal Aviation Administration (FAA), the number of flying Remotely Piloted Air Systems (RPASs), AKA drones, will increase rapidly. Challenges with drones not only concentrate on the security of these devices but also include criminal drone activity. Illegal drone operations are quickly growing, and criminals are continually developing new techniques and approaches. This research focuses on responding to criminal activity related to drones and examines some possible anti-forensic methods that criminals could use to alter digital evidence. The authors propose a forensic framework consisting of ten technical phases of analysis for UAV forensic artifacts that can reduce the complexity of the investigation. Furthermore, the authors explore the availability and value of digital evidence that would allow a more practical digital investigation to be able to build an evidence-based experience. Therefore, researchers focus on developing a technical drone investigation process that can be applied to several types of drones.

```
00 08 28 6D 6F 6F 76 00 00 00 6C 6D 76 68 64 00  ..(moov...lmvhd.
00 00 00 D5 A8 D8 82 D5 A8 D8 82 00 01 5F 90 00  ...ى_..ط,ض¨ط,ض¨.
01 5F EC 00 01 00 00 01 00 00 00 00 00 00 00 00  ._ى.............
00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00  ...@............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 03 00 00 00 80 75 64 74 61 00 00 00 28 46  .......€udta...(F
49 52 4D 33 2E 32 2E 33 34 28 41 29 00 00 00 00  IRM3.2.34(A)....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 28 43 41 4D 45 63 67 6F 33 67  ......(CAMEcgo3g
62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  b...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 53  ..............(S
45 54 54 00 00 00 28 58 14 D6 76 34 D0 83 3D 59  ETT...(X.ضv4ƒ=Y
8C D4 76 00 00 00 00 40 7E 42 01 2C 15 D6 76 A4  Œضv....@~B.,.ضv¤
9C 21 48 00 00 04 1B 74 72 61 6B 00 00 00 5C 74  œ!H....trak...\t
6B 68 64 00 00 00 07 D5 A8 D8 82 D5 A8 D8 82 00  khd....ط¨ض,ط¨ض,.
00 00 01 00 00 00 00 00 01 5F EC 00 00 00 00 00  .........ى_.....
00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 0F  ............@...
00 00 00 08 70 00 00 00 00 03 B7 6D 64 69 61 00  ....p.....·mdia.
00 00 20 6D 64 68 64 00 00 00 00 D5 A8 D8 82 D5  .. mdhd....ض,ض¨ض
A8 D8 82 00 01 5F 90 00 01 5F EC 00 00 00 00 00  ¨ط,ض..ط_..ى_....."
00 00 2B 68 64 6C 72 00 00 00 00 00 00 00 00 76  ..+hdlr........v
```

Figure 1- Content of 'udta' box

Timestamps are critical in forensics investigations. Therefore, extracting these timestamps will support the forensic analysis. As Figure 1 depicts, timestamps are found under the `moov' atom, which contains the `mvhd' and `udta' boxes.

1. The first box/atom indicates the file type, which is `MP42' at offset 0 – 24.
2. Then, there is `mdat' atom at offset 24 of size: 1481988989 bytes. The `mdat' atom usually contains media data of the video stream.
3. The `mvhd' atom starts at offset 1481989021 with a size of 108 bytes, and then the `udta' starts at offset 1481989129 with a size of 128 bytes. The `udta' atom contains two boxes, `FIRM' and `CAME.' information such as firmware version and camera type.

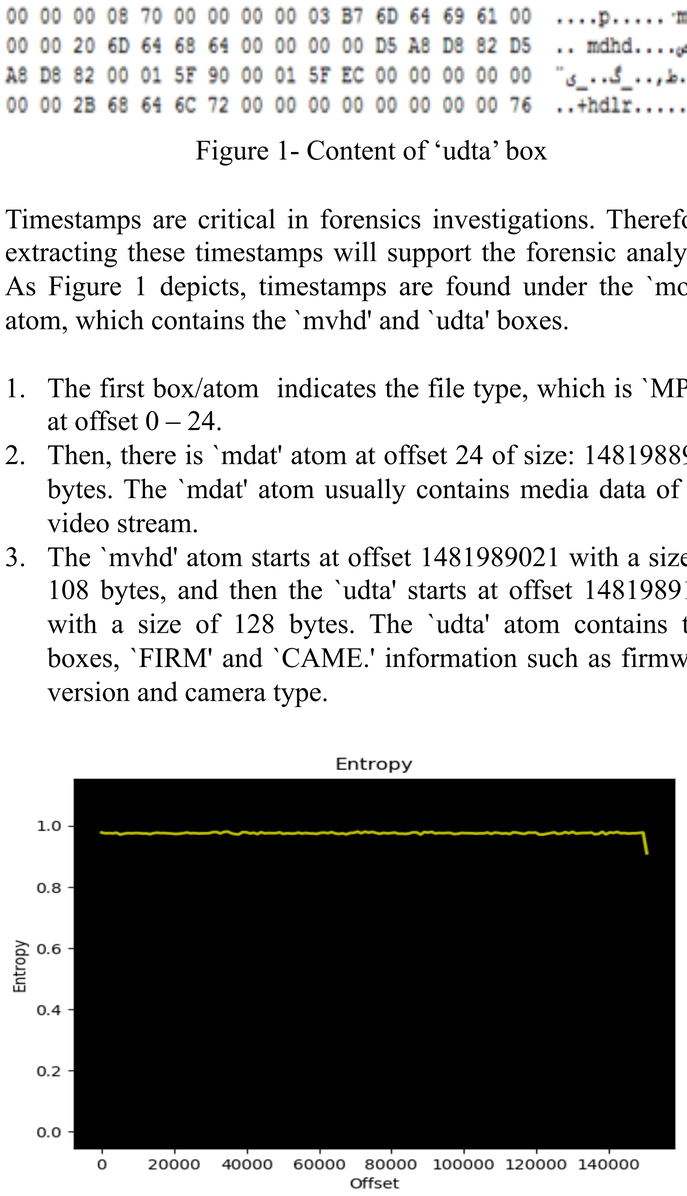

Figure 2- Entropy Evaluation of Typhoon -H Encrypted Flight Logs

The encryption mechanism of the Yuneec Typhoon H did not work properly especially on active flying mode which may lead to easy modification and further possible customization. Moreover, the encoded flight log is available under the unencrypted flight logs where it contains on-ground level data.

Drone Component	Media Files	Flight Logs	Event Logs	GPS Metadata	Sensor Logs	Flight Activity
Ground Station Controller	✔	✔	✔	✔	✔	✔
Mobile Device	✔			✔		✔
Memory Cards	✔					
Drone Chip-off			✔			

Table 1- Essential and non-essential digital evidence related to the drone

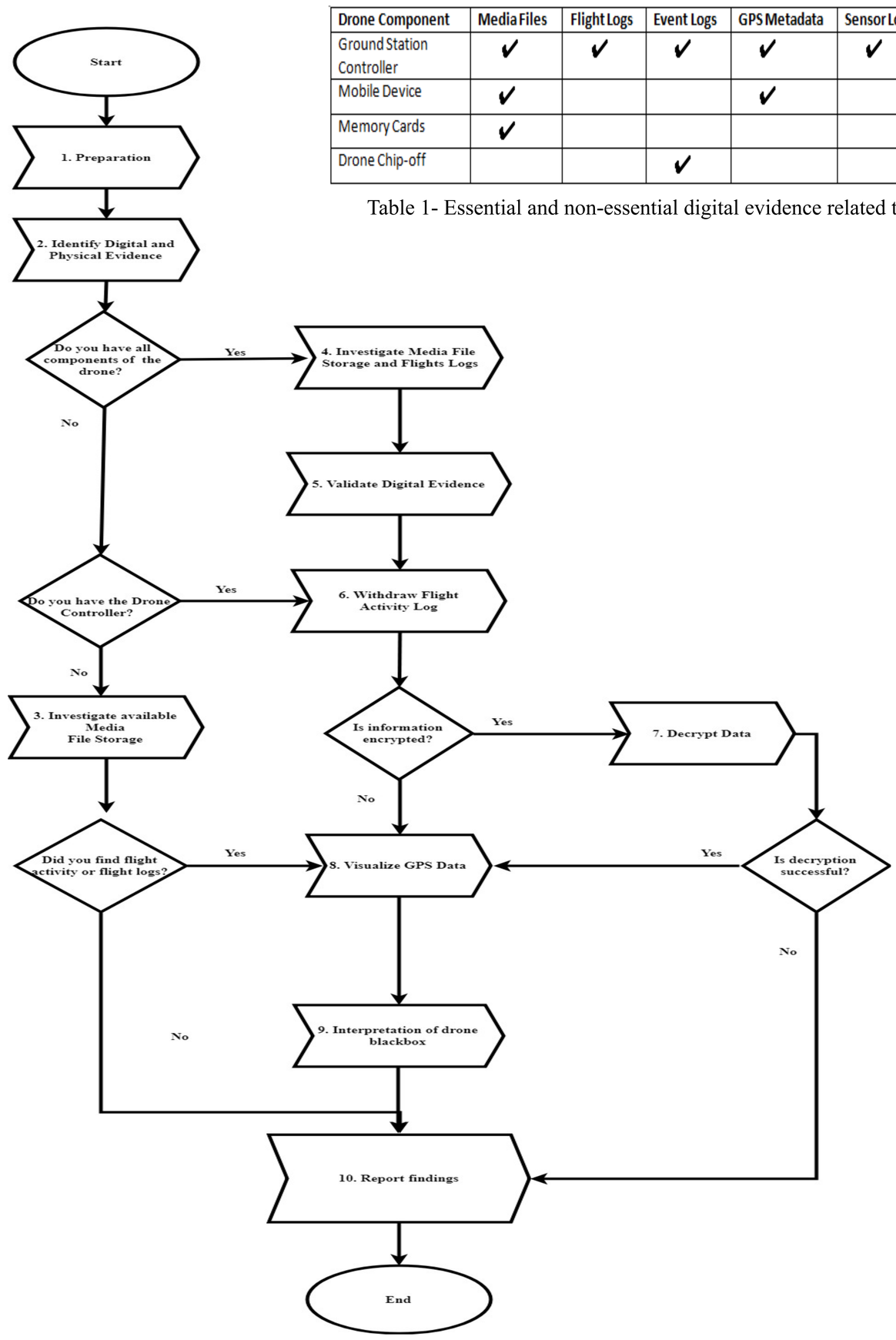

Figure 3- Proposed Drone Technical Forensic Investigation Process

Conclusion and Future Work

1. Researchers proposed ten technical investigative phases for forensic analysis of RPASs; where the Yuneec, Typhoon H used as a case study.
2. Future work can be done on other types of drones based on the proposed technical process, in order to develop a complete structure of drone forensics, and to generate more forensic tools to aid in automated investigation.
3. The current tool developed for research purpose only therefore, we welcome collaboration in developing the tool to be capable of other relevant features such as automatic interpretation of drone's black-box that is to the interest of forensic reporting.
4. We also aim to expand the drone incident response plan to include pre-incident and post-incident measures.