Forenzička analiza komercijalnih dronova

Jelena Gavrilović,Marko Tanasković, Miloš Stanković, Aleksa Ćuk
Tehnički fakultet
Univerzitet Singidunum
Beograd, Srbija
jgavrilovic@singidunum.ac.rs; mtanaskovic@singidunum.ac.rs; mstankovic@singidunum.ac.rs; acuk@singidunum.ac.rs

Sažetak— **Napredak tehnologije učinio je da dronovi postanu lako pristupačni svima. Ova tehnologija je značajno osvojila neke komercijalne organizacije i zbog toga je proizvodnja istih krenula drastično da raste. Sama komercijalizacija uvek ima za posledicu upotrebu dronova kako u humanitarne svrhe tako i u nezakonitim radnjama.**

U radu je prikazana upotrebu različitih metoda forenzičke analize na informacije dostupne u okviru samog drona kao i fizičkih tragova na samom dronu.

Pored komparativne analize metoda forenzičkih analiza bitno je istaći da je cilj rada da pokaže da li određeni podaci koji se ekstrakuju mogu da se koriste za kontrolu dronova.

Ključne riječi- digitalna forenzika, komercijalni dronovi, analiza podataka drona

I. UVOD

Dronovi su formalno poznatiji kao bespilotne letelice ili sistemi bespilotne letelice. Ono što ga izdvaja od ostalih letelica je da se može daljinski kontrolisati ili leteti autonomno koristeći softverski kontrolisane planove leta u svojim ugrađenim sistemima, koji rade u sprezi sa senzorima i globalnim sistemom pozicioniranja (GPS)

Pri nastanku ovakve letelice su najviše korišćene u vojnoj oblasti u razvijenim zemljama sve dok nije proširila svoju prepoznatljivost u javnosti i samim tim svoju dostupnost širom sveta.

Prisutna je velika zloupotreba dronova naročito jer je korisnicima data mogućnost modifikacije same letelice a sa druge strane pravni okvir ne definišu u potpunosti privatnost.

Ograničenja dronova koje se mogu zloupotrebiti:

1) Ne postoji standardizacija, svaki proizvođač ima svoje standarde izrade;
2) Postoji velika mogućnost izmena i podešavanja dronova;
3) Postojanje dronova koji nemaju funkciju beleženja podataka;
4) Postojanje dronova koji čuvaju podatke na uređaju(mobilnom telefonu) kojim su upravljani;
5) Identifikovanje neregistrovanih korisnika.

Rad je rezultat projekta #6524745, AI-DECIDE pod nazivom „Decentralized Machine Learning Control for Intelligent Multi-Agent Dynamical Systems“ koji je podržan od strane Programa razvoja veštačke inteligencije Fonda za nauku Republike Srbije.

Sa stanovišta digitalne forenzike drona, moguće je analizirali hardverske i softverske komponente. Istraga se tada svodi na ispitivanje fizičkih dokaza zajedno sa GPS lokacijom i svim multimedijalnim sadržajima koji su prikupljeni na mestu zločina.

II. KARAKTERISTE DRONA

A. *Detalji hardvera*

Dronovima obično upravljaju radio talasi od 2.4 gHz. Koriste kontroler koji može biti nalik *gamepad*-u *smart* telefona ili tableta. GPS čip prenosi svoju lokaciju na kontroler gde takođe belezi mesto poletanja u slučaju da treba da se vrati bez pomoći. Dronovi imaju vise rotora i propelera kako bi postigli nivo kontrole koji je neophodan da bi bili samostalni (*self- reliant*). Više propelera daje dronovima veću sigurnost. Ako jedan motor otkaže preostali motori održavaju letelicu mirnom u vazduhu. Što vise rotora imamo, veći će teret moći da podigne dron, na primer kameru.

B. *Načini komunikacije*

GPS pruža tačne podatke o položaju i lokaciji uređaja. WI-fi pruža mogućnost prenosa velike količine podataka do i od drona na određenom dometu. Bluetooth pruža još jedan način prenosa informacija do i od drona. 900Mhz/433MHz pruža komunikaciju dužeg dometa sa sporijom brzinom prenosa podataka.

Zapisi koje čuva dron nastaju na osnovu prepoznavanja pozicije, generišu se podaci neophodni za letenje drona i čuvaju u određenom čitljivom formatu. *System Data logs* je postao standard u većini modernih sistema i on funkcioniše kao crna kutija u avionima. Beleže se informacije sa nekih primarnih senzora drona, u te senzore spadaju: GPS, magnometer, akcelrometar, barometar, žiroskop, brzinomer, senzor i drugi.

III. FORENZIKA DRONA

U svojim počecima kada se nisu koristili nikakvi dodatni softverski alati, digitalna forenzika se zasnivala na tome da ispituje datoteke koje se generišu tokom leta, kao što su snimljeni podaci i operativni sistem koji koristi letelica i

evidentiranjem GPS lokacije koja bi se koristila kao dokaz u zločinu.

Sam proces sprovođenja digitalne forenzike je sastavljen iz faza: prikupljanje informacija, njihovog ispitivanja, analize i izveštavanja na osnovu dobijenih rezultata [1].

Prvi korak procesa odnosno faza prikupljanja podataka je jedino moguća ako se podaci prikupljaju iz izvora relevantnih podataka, sa nastojanjem očuvanja integriteta podataka. U skladu sa navedenim forenzika dronova se može obavljati kroz:

a) Forenziku dostupnih informacija i

b) Forenziku hardverskih komponenata drona

Forenzika dostupnih informacija ili digitalna forenzika predstavlja ispitivanje informacija putem mrežnih saobraćaja i mrežnih hostova. Ovaj sistem mreže uključuje i režim komunikacije dron - kontrolera. To podrazumeva kontroler za daljinsko upravljanje putem bežične komunikacije(radio signala) koristeći frekventne opsege. Zatim i analiziranje sistemskih logova (uključujući i očitavanje senzora na letelici), sistema za skladištenje podataka kao i snimke sa kamere.

Hardverska forenzika uključuje: identifikovanje tipa drona, proveru prilagođavanja (*customization*), nošenje tereta, otiske prstiju i lokaciju.

A. Parametri drona koji se proveravaju

Trenutno jedni od važnijih parametara koji su čitljivi su: status letelice, geografske širine i dužine, datum i vreme, inercijalna merna jedinica (IMU), kompas, pređena udaljenost, brzina, visina, snaga i struja, tip komunikacije između drona i kontrolera, snimci kamera. Neki od sačuvanih parametara mogu biti korisni za forenzičku analizu poput serijskog broja kamere i baterije, tip mobilne aplikacije, tip drona, broj snimljenih fotografija, vreme snimanja, itd.

Kada se govori o rotacija dronova , parametri kotrljanja, nagiba i skretanja su odgovorni za osnovnu kretnju odnosno rotaciju poput svih avio letelica. JavaFX 8 je platforma zasnovana na java programiranju desktop aplikacija. Ona pruža bogati grafički prikaz za dizajn igara i grafikona. Upravo po dobro poznatoj implementaciji 3D grafičkog prikaza, JavaFX8 klasa Animation je pomogla da se uspešno reprodukuje animacija kao što je u ovom slučaju rotacija i samim tim kretnja dronova.

Provera otisaka prstiju: Svaki dron ima odvojivu bateriju i propelere kao i još dodatne komponente za pričvršćivanje. Stoga, otisci prstiju se mogu naći na čvrstoj površini drona poput baterije, nosivosti i blizu krila [2].

Provera nosivosti: Najveći broj zločina u vezi sa dronovima uključuje nošenje ilegalnih predmeta kao što su oružje, telefoni i narkotici. Dakle, predmet razmatranja nije bruto težina drona nego ukupna predviđena izdržljivost. Komercijalno dostupni dronovi danas mogu da podignu težinu od 4g do 18kg, dok teretni dronovi mogu podići čak do 1814kg.

Provera delova (komponenti drona): Svaka komponenta broja ima svoj identifikacioni broj. Serijski brojevi na bateriji, kontroleru leta, kameri, GPS uređaju, propelerima i motorima uključujući i naziv proizvođača sa datumom proizvodnje, prenosi mnogo informacija.

U samom radu analizirani su sledeći dronovi, koji su od istog proizvođača ali različitih karakteristika. Njihova specifikacija je data u Tabeli 1 [10]

TABELA I. UPOREDNE KARAKTERISTIKE DRONOVA

TIP	DJI Mavic Air 2 Fly More Combo	DJI Mavic 2 Enterprise Dual
Tezina:	570g	900g
Dimenzije:	183×253×77 mm	322×242×84 mm
Maksimalna brzina (bez vetra):	19 m/s	72 km/h
Maksimalna operativna visina	5000 m	6000 m
Interna memorija	8 GB	24 GB
Satelitski sistemi:	GPS+GLONASS	GPS+GLONASS
Senzori:		Omnidirectional Obstacle Sensing
Kamera	Vizuelna kamera (Effective pixels: 12M and 48M, FOV: 84°, Aperture: f/2.8, Focus: 1 m to ∞, ISO Range Video: 100-6400, Photo: 100-1600, Max Image Size: 8000×6000 (4:3), Video Recording Modes 4K Ultra HD: 3840×2160 60p, 2.7K: 2688×1512 60p, FHD: 1920×1080 240p, Max Video Bitrate 120 Mbps)	Termalna Kamera (HFOV: 57°, Aperture: f/1.1, Sensor Resolution 160×120, Spectral Band 8-14 μm) Vizuelna kamera (Effective pixels: 12M, FOV: approx. 85°, Aperture: f/2.8, Focus: 0.5 m to ∞, ISO Range Video: 100-12800, Photo: 100-1600, Max Image Size: 4056×3040 (4:3); 4056×2280 (16:9), Video Recording Modes 4K Ultra HD: 3840×2160 30p, 2.7K: 2688×1512 30p, FHD: 1920×1080 30p, Max Video Bitrate 100 Mbps)

B. Digitalna forenzika drona

Dronovi svoje log fajlove čuvaju u različitim formatima kao sto su (.csv), (.txt) ili (.dat); .dat fajlovi su uglavnom podeljeni na 2 vrste [3]. Prva vrsta čuva binarne podatke koje može dekodirati samo aplikacija koja ih je generisala, dok je druga vrsta u stvari *text-based data file* koji se može pregledati korišćenjem nekog *text* editora. U ovom istraživanju je bio potreban *Keyhole Markup Language(.kml)* za vizuelizaciju putanje leta preko Google-ovog KML API-a.

KML datoteke sadrže XML oznake koje predstavljaju geografske anotacije. Ovaj format datoteke pomaže u pronalaženju određenih lokacija na mapi, geometrijskih oblika, 3D modela, slika itd. I zbog toga se može tacno locirati putanja leta nekog drona. Postoji KML File konverter koji je dostupan online [link].

Oba drona čuvaju svoje log fajlove u dat formatu. Kako finalni fajl treba da bude u KML formatu kreiran je prilagodljivi CSV-to-KML konverter koji je kompatibilan sa API-jem.

Konverter bira potrebne parametre i daje im odgovarajuće XML tagove i tako generise KML datoteku za zadati log fajl. Zatim se ta generisana KML datoteka koristi za predstavljanje putanje leta drona u aplikaciji.

1) Procedura dobijanja logova

Proizvođač dronova postavlja metod za izvlačenje informacija o evidenciji leta. Za neke dronove potrebno je izvaditi samo memorijsku karticu i iz nje saznati sve podatke dok drugi zahtevaju prenos podataka iz aplikacije koja se nalazi u telefonu korisnika.

Dronovi koji se analiziraju su od istog proizvođača različitih karakteristika, Iako je način za izvlačenje *flight log-ova* (protokol o letu), jednostavniji kod drugih proizvođača broj parametara koji su dostupni u okviru logova je mnogo veći kod DJI drona. [4] Ne čuva svoje *flight logove* u sebi već ih direktno šalje na svoj St-16 kontroler koji radi na Android OS-u i tim fajlovima može pristupiti putem regularnog android fajl sistema.

Takođe ima MicroSD karticu od 32 GB koja služi kao log saver. Postoji i USB port na dnu kontrolera koji se koristi za povezivanje na računar kako bi svi podaci bili prebačeni i spremni za pregled. Ovaj dron sve svoje log fajlove čuva u .csv formatu koji su smešteni u vise direktorijuma pod nazivom Remote, Remote GPS, Sensor i Telemerty.

IV. REZULTATI

Pre same analize kroz različite podatke, bitno je naglasiti da se informacije čuvaju u različitom formatu u svakom dronu i sadrže razne važne parametre koji se odnose na let koji vrši dron.

DJI evidencije letova se čuvaju u.DAT formatu koji je šifrovan. Dnevnici letenja kod nekih dronova se lako mogu otvoriti uz pomoć bilo kog uređivača teksta kao što je notepad. Različiti formati koji se koriste za skladištenje informacija utiču direktno na vreme potrebno za analizu logova. Analiziranje je kompleksije kako sami zapisi pripadaju letu dužem od 5 min. Količina zapisa se prilikom ovakvih letova eksponencijalno povećava.

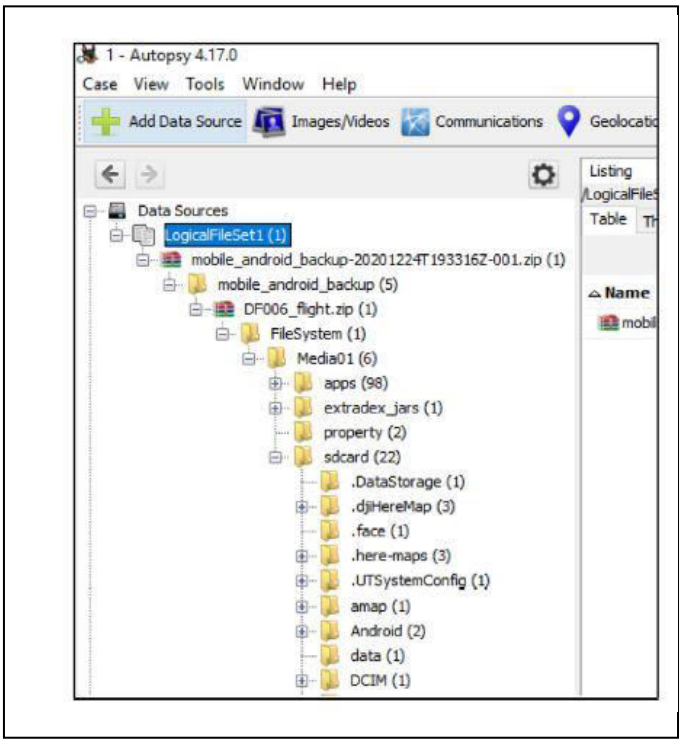
Po tipu i serijskom broju se dronovi takođe razlikuju jedni od drugih iako je isti proizvođač. DJI čuva brojne parametre kao što su evidencija pozicioniranja, nadmorska visina, relativna visina, apsolutna visina, roll-pitch-iav detalji, ubrzanje u k, i & z smeru, žiroskop zapisi, brzina, brzina itd. Broj različitih sačuvanih parametara od DJI drona ide do 268.

Pored velikog broja parametara koje se generišu kod DJI dronova pri samom letu, takođe, generišu se logovi od strane kontrolora leta drona tokom svakog leta. Ovaj podatak je jako bitan jer se povećava broj unosa informacija u dnevnik u sekundi, precizniji i tačniji su podaci dnevnika leta. Analiza ovako preciznog artefakta može biti od veliki značaj pri sprovođenju kompletne forenzičke istrage na dronu.

Postoji mogućnost rekonstrukcije putanje leta u alatu Google Earth Pro, putanja leta se prikazuje u 2D obliku kao iz ptičje perspektive. Drugi dimenzija odnosno visina u odnosu na početnu tačku je takođe veoma važno za vizuelizaciju putanje leta. Ovo može pomoći u procesu analize za bolje razumevanje putanje leta. Kada je putanja leta konstruisana korišćenjem GPS podataka analizira se zajedno sa nadmorskom visinom grafa, pruža detaljnije informacije o letu drona.

Logički metod akvizicije podataka zahteva da baterija drona bude dovoljno napunjena. DJI Assistant Aplikacija sa OEM veb lokacije mora biti instalirana na računar. Nakon instaliranja i pokretanje aplikacije DJI Assistant 2 i kreiranje besplatnog DJI naloga, dron treba da bude uključen i mora da bude povezan na računar pomoću Micro-USB kabla. Ikona drona se pojavljuju u aplikaciji DJI asistenta. Logovima se sada može pristupiti sa interne SD kartice drona.

Zip datoteka je uvezena u alat za digitalnu forenziku pod nazivom Autopsy. U okviru alata korišćen je modul pod nazivom „Embedded File Ektractor“. Uvežena datoteka sa strukturom direktorijuma i hijerarhijom prikazana je na Slici 1



Slika 1. Analiza drona uz pomoć Autopsy

U analizi pomoći alata Autopsy različiti podaci mogu biti dostupni, ono što je bitno naglasiti je da kako se analizira sama memorija kroz različite module u okviru softvera, tako se mogu povratiti i obrisani podaci.

V. ZAKLJUČAK I BUDUĆA ISTRAŽIVANJA

Cilj rada je bio izdvajanje i analiza različitih podataka koji se mogu koristi za forenziku dronova. Kako se forenzika kao nauka vezuje za događaje koji se su desili i sami podaci moraju biti takvi da se prilikom analize iz njih mogu definisati pravosnažni dokazi.

Ovim radom je pokazano da svi podaci koji se dobijaju na različite načine iz dronova, mogu biti dokazi koji se mogu smatrati relevantnim.

Autori rada na projektu finansiranom od fonda za nauku Republike Srbije kao jedan od ciljeva samog projekta DECIDE imaju i razvijanje hardverskih i softverskih rešenja za dva specifična problema: autonomno upravljanje rojem bespilotnih letelica u misiji pretrage i otpreme korisnog tereta i inteligentno decentralizovano upravljanje proizvodnom linijom.

Ovaj rad treba da pokaže koje su karakteristike dronova i da li ekstraktovni podaci mogu biti u budućim istraživanjima pomoćni podaci za treniranje softverskih rešenja.

LITERATURA

[1] Azhar, M.A.H.B., Hannan, A., Barton, T., Islam, T.: Drone forensic analysis using open source tools. J. Digit. Forensics Secur. Law 13(1), 6 2018.

[2] Ali, K.M.: Digital forensics best practices and managerial implications. In: 4th International Conference on Computational Intelligence, Communication Systems and Networks, CICSyN, pp. 196–199.

[3] Iqbal, F., Alam, S., Kazim, A., MacDermott, Á.: Drone forensics: a case study on DJI phantom 4. In: IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, pp. 1–6 2019.

[4] Finn, R.L., Wright, D.: Privacy, data protection and ethics for civil drone practice: a survey of industry, regulators and civil society organisations. Comput. Law Secur. Rev. **32**, 577–586 2016.

[5] Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., Witten, I.H.: The weka data mining software: an update. SIGKDD Explor. News **11**, 10–18 2009.

[6] Mekala, S.H., Baig, Z.: Digital forensics for drone data – intelligent clustering using self organising maps. In: Doss, R., Piramuthu, S., Zhou, W. (eds.) FNSS 2019. CCIS, vol. 1113, pp. 172–189. Springer, Cham 2019.

[7] United States Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) 2018, The Drone Forensic Program, VTO Inc. Accessed 20 Mar 2020.

[8] Hartmann, K., Giles, K.: UAV exploitation: a new domain for cyber power. In: Pissanidis, N., Rõigas, H., Veenendaal, M. (eds.), 8th International Conference on Cyber Conflict: Cyber Power, pp. 205–221 (2016).

[9] Vattapparamban, E., Güvenç, İ., Yurekli, A.İ., Akkaya, K., Uluağaç, S.: Drones for smart cities: issues in cybersecurity, privacy, and public safety. In: International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, pp. 216–221 (2016),

[10] https://www.dji.com/

ABSTRACT

Advances in technology have made drones easily accessible to everyone. This technology has won over some commercial organizations and this caused a significant increase in the production of drones. The commercialization has resulted in the use of drones both for humanitarian purposes and illegal activities.

The paper presents the use of different methods of forensic analysis on information available from the drone as well as on information gathered from physical traces on the drone itself.

In addition to comparative analysis of forensic analysis methods, it is important to point out that the aim of this paper is to show whether certain extracted data can be used to control drones.

FORENSIC ANALYSIS OF COMMERCIAL DRONES

Jelena Gavrilović,Marko Tanasković, Miloš Stanković, Aleksa Ćuk