Forenzička analiza sustava bespilotnih zrakoplova

Kletuš, Tomislav

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:051183

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Tomislav Kletuš

FORENZIČKA ANALIZA SUSTAVA BESPILOTNIH ZRAKOPLOVA

DIPLOMSKI RAD

Zagreb, rujan 2020.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 1. travnja 2020.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Forenzička analiza informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 5892

Pristupnik: **Tomislav Kletuš (0135236817)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Forenzička analiza sustava bespilotnih zrakoplova**

Opis zadatka:

Odrediti značajke komercijalnih bespilotnih zrakoplova kao terminalnih uređaja. Objasniti regulatorni aspekt operativne primjene bespilotnih zrakoplova u RH. Opisati mogućnosti sigurnosnih protumjera letačkim aktivnostima bespilotnih zrakoplova. Definirati metodologiju ekstrakcije podataka s bespilotnih zrakoplova i njima povezanih elemenata. Analizirati ekstrahirane podatke sustava bespilotnih zrakoplova.

Mentor:

dr. sc. Siniša Husnjak

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

FORENZIČKA ANALIZA SUSTAVA BESPILOTNIH ZRAKOPLOVA

FORENSIC ANALYSIS OF UNMANNED AERIAL VEHICLE SYSTEM

Mentor: dr. sc. Siniša Husnjak

Student: Tomislav Kletuš
JMBAG: 0135236817

Zagreb, rujan 2020.

SAŽETAK

Ekspanzijom korištenja bespilotnih zrakoplova te njihovom rastućom primjenom u raznolikim industrijama, s obzirom na njihove karakteristike isti postaju interesantni u području digitalne forenzike zbog mogućnosti zlouporabe. Kako je za upravljanje i korištenje značajki bespilotnih zrakoplova često potrebna letačka aplikacija na mobilnom uređaju, u forenzičkom smislu mobilna forenzika postaje vrlo slična forenzici bespilotnih zrakoplova. Tim dvjema granama digitalne forenzike u jednom istraživačkom postupku, odabirom valjanih metoda i alata može se prikupiti značajan skup podataka. Najveće izazove predstavljaju nedovoljno standardizirane metodologije i postupci u izvođenju ekstrakcije, nedorečenost zakonskih akata, regulative te sofisticirane protumjere letačkim aktivnostima. Radom je dan pregled pristupu forenzičkoj istrazi komercijalnog bespilotnog zrakoplova unutar scenarija nezakonitih aktivnosti korištenja bespilotnog zrakoplova. Također, na složenost istrage utječu faktori poput odabranih alata, metoda te korištenih mobilnih uređaja kojih je za veću uspješnost ekstrakcije i analize potrebno imati u što većem opsegu. Trenutno ne postoji standardiziran smjer pristupu digitalnoj forenzici bespilotnih zrakoplova te kombinacija različitih alata daje najbolje rezultate što se često očituje kroz dugotrajni sudski postupak.

KLJUČNE RIJEČI: bespilotni zrakoplov; mobilni uređaj; ekstrakcija podataka; forenzički alat; digitalna forenzička analiza

SUMMARY

With the expansion of the use of unmanned aerial vehicles and their growing application in various industries, given their characteristics, they are becoming interesting in the field of digital forensics due to the possibility of its criminal abuse. As the flight application on a mobile device is often required to manage and use the drones and its features, in forensic terms mobile forensics is becoming very similar to the forensics of drones. With these two digital forensics branches, a significant set of data can be collected by validly selected methods and tools. The biggest challenges are insufficiently standardized methodologies and procedures in performing extraction, vagueness of legal acts, regulations and sophisticated countermeasures to flying activities. The paper provides an overview of the approach to forensic investigation of a commercial unmanned aircraft within the scenario of illegal activities of its use. Also, complexity of the investigation is influenced by factors such as selected tools, methods and used mobile devices, which for greater extraction and analysis success it is recommended to have as much as possible. Currently, there is no standardized approach to digital drones forensic for drones. Combination of different forensic tools gives the best results, which is unfortunately reflected in the lengthy court proceedings.

KEY WORDS: Drone/UAV; mobile device; data extraction; forensic tool; digital forensic analysis;

Sadržaj

1. Uvod 1

2. Značajke komercijalnih bespilotnih zrakoplova kao terminalnih uređaja 3

2.1. Karakteristike i elementi bespilotnih zrakoplova 5

2.2. Karakteristike bespilotnog zrakoplova DJI Mavic Air 9

2.3. Potencijalni izvori podataka prema elementima ekosustava bespilotnih zrakoplova 12

3. Regulatorni aspekt primjene bespilotnih zrakoplova u RH 17

3.1. Zakonski okvir operativne primjene bespilotnih zrakoplova u RH 17

3.2. Zakonski okvir pri aktivnostima snimanja iz zraka u RH 22

3.3. Statistički trendovi primjene bespilotnih zrakoplova u RH 26

4. Sigurnosne protumjere letačkim aktivnostima bespilotnih zrakoplova 28

4.1. Detektiranje bespilotnog zrakoplova 30

4.2. Mehanizmi zaustavljanja bespilotnog zrakoplova 32

5. Metodologija i metode akvizicije podataka s bespilotnih zrakoplova 36

5.1. Referentna metodologija mobilne digitalne forenzike 37

5.2. Metode ekstrakcije digitalnih dokaza 40

6. Forenzička analiza bespilotnog zrakoplova DJI Mavic Air 45

6.1. Akvizicija podataka s DJI Mavic Air 48

6.2. Akvizicija podataka sa Sony Xperia Z1 49

6.3. Analiza ekstrahiranih podataka 50

6.3.1. Analiza podataka dostupnih ručnom navigacijom uređaja 50

6.3.2. Analiza podataka dohvaćenih Cellebrite UFED Touch 2 54

7. Zaključak 61

Popis literature 62

Popis kratica 68

Popis slika 71

Popis grafikona 72

Popis tablica 73

1. Uvod

Razvojem tradicionalnih letjelica, jedan od tehničkih zahtjeva čovječanstva je bilo stvoriti letjelicu bez direktno-upravljačkog ljudskog faktora tj. pilota, s ciljem korištenja u raznim granama poslovnih i društvenih aktivnosti. Značajnim napretkom tehnologije u vidu elektronike, računalstva te informacijsko-komunikacijskih sustava omogućeno je ostvarivanje ideje o letjelicama upravljanim na daljinu tj. bespilotnim zrakoplovima. Prvotna ideja razvitka takvih letjelica te implementacija istih stigla je iz vojnih krugova za njihove potrebe i svrhe pod kraticom UAV (engl. *Unmanned Air Vehicles*), tj. bespilotni zrakoplovi, letjelice - dronovi. Tehnološkim sazrijevanjem, uočen je njihov potencijal za unaprjeđenje te olakšavanje djelatnosti u drugim područjima poput traganja i spašavanja, nadzora, građevine, prometa i transporta, poljoprivrede te rekreacije.

Važno je razumjeti kako sve veći rast sustavnog procesa ponude i potražnje dovodi do širenja različitih bespilotnih zrakoplova (engl. *drones*) na tržištu uz drastičan pad njihove cijene. Sukladno tome, isti su se komercijalno približili privatnim korisnicima što su prepoznale kriminalne organizacije i kriminalci te su ih odabrali kao produženi alat za izvršavanje svojih aktivnosti. Upravo iz tog razloga, bespilotni zrakoplovi su postali izuzetno zanimljivi istražiteljima, pogotovo u području digitalne forenzike o kojoj se ne zna još puno te nije toliko raširena javna spoznaja o njoj. Današnje komercijalne bespilotne zrakoplove može se poistovjetiti sa zračnim kamerama i mobilnim terminalnim uređajima što sadržaj njihove memorijske pohrane čini vrlo primamljivim i zanimljivim digitalnim forenzičarima.

Naslov i tema ovog diplomskog rada je *Forenzička analiza sustava bespilotnih zrakoplova*, a cilj rada je proširiti spoznaje o tome što bespilotni zrakoplovi predstavljaju u disciplini digitalne forenzike te na koji način je moguće dohvatiti i analizirati sadržaj njihove pohrane unutar spektra njezinih djelatnosti. Točnije, mogućnosti ekstrakcije i analiza dohvaćenih podataka bit će provedene na bespilotnom zrakoplovi tvrtke DJI, modelu Mavic Air. Diplomski rad sastoji se od sedam cjelina:

1. Uvod
2. Značajke komercijalnih bespilotnih zrakoplova kao terminalnih uređaja
3. Regulatorni aspekt primjene bespilotnih zrakoplova u RH
4. Sigurnosne protumjere letačkim aktivnostima bespilotnih zrakoplova
5. Metodologija i metode akvizicije podataka s bespilotnih zrakoplova
6. Provedba forenzičke analize bespilotnog zrakoplova DJI Mavic Air
7. Zaključak

U drugom poglavlju bit će predstavljeni osnovni ključni pojmovi, kratak opis razvoja te značajke bespilotnih zrakoplova kroz njihove izvedbene elemente, mogućnosti primjene te načine kojima se njima upravlja. Također, ovo poglavlje sadržavat će informacije o tome koje sličnosti dijele bespilotni zrakoplovi s pametnim mobilnim terminalnim uređajima s obzirom na komunikacijske tehnike, sklopovlje, pohranu i obradu podataka. Uz karakteristike, iznijet će se potencijalni izvori digitalnih dokaza prema pojedinom elementu ekosustava bespilotnog zrakoplova.

Treće poglavlje sadržavat će opise regulativa Republike Hrvatske kojima se ponajprije utvrđuje njihova operativna primjena te zakonodavnog okvira tj. pravilnika kojim se propisuju pravila, zabrane, mogućnosti i obaveze pilota na daljinu pri snimanju iz zraka. Navedeno će biti objašnjeno kroz konkretan primjer korištenja DJI Mavic Air bespilotnog zrakoplova. Kao dopuna, bit će izneseni statistički podaci o korištenju i samoj operativi bespilotnih zrakoplova u Republici Hrvatskoj.

Načini pristupanju problemu zaštite i obrnuto-sigurnosnom djelovanju bespilotnim zrakoplovima bit će izneseni u četvrtom poglavlju. Ono će sadržavati načine pripreme, detekcije, odvraćanja te zaustavljanje i uništavanja bespilotnih zrakoplova u svrhu sprječavanja sigurnosnih incidenata, popraćeno primjerima koji su u trenutnoj uporabi.

Predstavljanje referentne forenzičke metodologije, principa dohvaćanja podataka s bespilotnog zrakoplova koju su istovjetni forenzičkoj istrazi pametnih mobilnih uređaja putem određenih forenzičkih alata bit će obrađeno u petom poglavlju. Ono, uz iduće šesto poglavlje, tvori temeljni dio rada zbog forenzičke zvučnosti i usmjerenosti prema toj disciplini.

U šestom poglavlju bit će analizirane mogućnosti i izazovi korištenih forenzičkih alata u procesu ekstrakcije digitalnih dokaza s bespilotnog zrakoplova DJI Mavic Air, kao i detaljno raščlanjivanje memorijske slike tj. skupa podataka i metapodataka dobivenih u tom procesu.

2. Značajke komercijalnih bespilotnih zrakoplova kao terminalnih uređaja

Gledajući širu sliku, sve bespilotne letjelice tj. bespilotni zrakoplovi mogu se okarakterizirati kao jedan cjelovit sustav, suprotan svim direktno upravljivim letjelicama, pod nazivom UAS (engl. *Unmanned Aerial System*). Kako je rečeno u uvodu, glavni akronim koji opisuje sve bespilotne zrakoplove je UAV (engl. *Unmanned Air Vehicles*), a on se odnosi na svaki tip letjelice koja ostvaruje kretanje zračnim prostorom bez pretpostavljenog ljudskog faktora u vidu izravnog upravljanja, tj. pilota. U tu kategorizaciju ulaze i razni zrakoplovi kojima se upravlja na daljinu te ostale letjelice koje su namijenjene za potpuno samostalno i automatizirano kretanje kroz zračni prostor prema nekim prethodno utvrđenim (programiranim) parametrima.

Sve većim razvojem tehnologije i takvih letjelica, došlo je do pojave tzv. multikoptera/multirotora, popularnijih pod engleskim sinonimom *drone*, koji ovisno o svojoj konstrukciji imaju najčešće četiri ili više elektro-motora pomoću kojih ostvaruju polijetanje, sam let i slijetanje uz pomoć rotacijskih krilaca, odnosno propelera te su po njima dobili naziv.

Oni su izvedbeno i vizualno sličniji helikopterskim letjelicama nego zrakoplovima s fiksnim krilima koji su u pravilu kompleksniji, skuplji, imaju veći dolet i nosivost ali i smanjenju agilnost dok im je namjena uglavnom profesionalne prirode. Uz njih, na tržištu se pojavljuju i hibridne letjelice koje kombiniraju značajke multikopter i izvedbe fiksnih krila tzv. VTOL (engl. *Vertical Take Off and Landing*) sustavi bespilotnih zrakoplova. Oni imaju mogućnost agilnijih zračnih manevara uz zadržavanje velikog doleta.

Multikopter bespilotni zrakoplovi najrašireniji su u poslovnoj i komercijalnoj korisničkoj skupini. Glavna razlika naprema bespilotnih zrakoplova s fiksnim krilima je njihova veća brzina, okretnost, laka upravljivost, vertikalno uzlijetanje i slijetanje te mala ili nikakva nosivost uz kratko vrijeme provedeno u zraku. Isti su upravljivi na daljinu te njihov operator, pilot koristi neku vrstu upravljača za njihovo manevriranje, [1], [2].

Upravljači, tj. kontroleri su danas najčešće posebno izrađeni za individualne modele i marke dronova ili su pak izvedeni kombinacijom upravljačke aplikacije i nekog mobilnog terminalnog uređaja (pametni mobilni telefon, tablet uređaj i sl.) na kojem je takav upravljačka aplikacija instalirana.

Iz tog razloga ovakvi dronovi, bespilotni zrakoplovi često su opisani akronimom RPAS (engl. *Remotely Piloted Aircraft System*). Kod RPAS bespilotnih sustava, isti se sastoji od zemaljske GCS (engl. *Ground Control System/Station*) stanice te same letjelice. Njihova komunikacija se odvija najčešće putem radio-valova kroz zrak kao komunikacijski medij unutar određene komunikacijske tehnologije, primjerice poput *Wi-Fi* (IEEE 802.11 standard) ukoliko se bespilotnim zrakoplovom upravlja direktno putem pametnog

terminalnog uređaja (gdje je *Wi-Fi* veza potrebna samo za uparivanje bespilotnog zrakoplova i pametnog mobilnog uređaja ali ne i za letenje) ili neke druge *proprietary* RC (engl. *Radio Communication*) tehnologije između upravljača i bespilotnog zrakoplova , [1], [2].

Slika 1. Izvedbe multikopter/multirotor bespilotnih zrakoplova, [3]

Osnovni fizički dijelovi svakog bespilotnog zrakoplova, koji mu omogućavaju kretanje zračnim prostorom, odnosno let su: letački pogon (propeleri i rotori), tijelo i platforma (oprema za uzlet i slijetanje - postolje), posebno izrađeni softver (operativni sustav), hardver (matična ploča tj. kontrolor leta i komponente, antenski sustav, vanjska memorijska pohrana), dodatni senzori (žiroskop, akcelerometar, magnetometar, senzori za sprječavanje kolizije, senzori protoka zraka, električni kompas, GNSS – *Global Navigation Satellite System*) senzori, kamera te pogonsko napajanje (ugrađena ili eksterna baterija). Današnje bespilotne zrakoplove, s obzirom na pripadajuće elemente može promatrati kao mobilne terminalne uređaje, zato što zbog svojih karakteristika, omogućuju povezivanje s drugim pametnim uređajima te međusobnu komunikaciju ujedno uz prikupljanje, obradu i distribuciju podataka dobivenih kroz senzore iz vlastite letne okoline, [4], [5].

Bespilotne zrakoplove može se u grubo prema namijeni podijeliti na vojne i civilne, od kojih su za sama znanstvena istraživanja važnije spoznaje o civilnima čija je dostupnost široj javnosti zadnjih nekoliko godina porasla zbog pada cijena na nekoliko stotina američkih dolara.

Stoga prema izvoru Hrvatske agencije za civilno zrakoplovstvo (engl. CCAA – *Croatian Civil Aviation Agency*) [6], te prema izvoru američkog ministarstva obrane i federalne zrakoplovne agencije [7], današnji se bespilotni zrakoplovi tehnički mogu kategorizirati prema sljedećim karakteristikama koje su potrebne za sigurno i legalno izvođenje letačkih aktivnosti te njihovo upravljanje općenito:

I. Maksimalna brzina leta – najveća tvornička brzina letenja drona
II. Operativna masa – masa drona u trenutku upravljanja i letačke aktivnosti

2.1. Karakteristike i elementi bespilotnih zrakoplova

Elementi i ostale fizičke komponentne bespilotnog zrakoplova koje su izravno vezane uz njegovo funkcioniranje razlikuju se što izgledom što operativno te ovise o pojedinom modelu i proizvođaču bespilotnog zrakoplova te ponajviše prema želji krajnjeg korisnika tj. pilota na daljinu i njegovom načinu korištenja. Karakteristike su najčešće određene prema namijeni, čija podjela bespilotnih zrakoplova može biti prema sljedećem:

a. Rekreacijski bespilotni zrakoplovi
   Očituje ih niska cijena, koriste se kao igračke od strane djece, amatera i entuzijasta, često su karakteristikama ograničeni na let u zatvorenom prostoru, osnovni hardverski i softverski sustav.

b. Komercijalni bespilotni zrakoplovi
   Proizvođači ih isporučuju s osnovnom i dodatnom opremom koja se koristi za utvrđivanje krajnje namjene poput osnovnog letačkog pogona te dodatnih senzora npr. kamere za snimanje i fotografiranje iz zraka. Razlika ovakvih tipova bespilotnih letjelica u odnosnu na rekreacijske nije u karakteristikama već krajnjoj primjeni, koja u ovom slučaju zbog dodatne opreme može biti i komercijalna što utječe na njihovu višu cijenu.

c. Tzv. „Uradi sam“ bespilotni zrakoplovi
   To su DIY (engl. *Do It Yourself*) bespilotni zrakoplovi osmišljeni i izrađeni prema željama i potrebama korisnika, bilo u vlastitom angažmanu ili uz pomoć drugih proizvodnih strana. Od rekreacijskih i komercijalnih bespilotnih zrakoplova razlikuje ih korištenje posebnih dijelova i komponenti koji zasebno mogu ili ne moraju biti predodređeni za korištenje u sustavu bespilotnog zrakoplova te su kao takvi unikatni i ne proizvode se serijski. Cjenovno i karakteristikama variraju, što ponajviše ovisi o željama i potrebama krajnjeg korisnika te mogu biti ograničeni dostupnošću pojedinih elemenata na tržištu kao i potrebnom stručnošću, znanjem za njihovu izradu. Kao takvi, mogu biti izrađeni u jednostavnim izvedbama poput rekreacijskih ili pak složenijim izvedbama poput komercijalnih bespilotnih zrakoplova.

Svaka prethodna namjenska kategorija izrađena je od nekih elemenata koji su opisani u nastavku kroz fizičke komponentne, [2], [4], [8]. Letni sustav i njemu pripadajuća mehanika je poveznica koju dijele dok su dodatna oprema ili bolje letne karakteristike glavna razlika.

I. Fizičke komponentne/hardver

Okvir – kućište, najčešće izrađeno od plastičnih polimera ili materijala od karbonskih vlakana. Ono sadrži sve ostale hardverske komponente te ih štiti od izravnih vanjskih utjecaja.

Kontroler leta – elektronička komponentna bespilotne letjelice koja služi za upravljanje ostalih komponenti povezanih na nju, u računalnoj analogiji on bi predstavljao matičnu ploču s pripadajućom upravljačko-procesorskom jedinicom. U njemu se obrađuju navigacijske naredbe pristigle s daljinskog kontrola, upravljača te iste pretvara u letne aktivnosti bespilotnog zrakoplova. Naredbe koje obrađuje može primati u stvarnom vremenu ili iste mogu biti tvornički programirane kako bi se omogućile određene autonomne funkcije leta.

Letni pogon – tu spadaju motori, propeleri te kontroleri brzine tzv. ESC (engl. *Electronic Speed Controllers*). Njihovo zajedničko djelovanje zaslužno je za uzlijetanje, let te slijetanje bespilotnog zrakoplova te njegovo lebdenje i zadržavanje u zraku. Dok su ispravni propeleri i motori važni za temeljne letne operacije, određivanje smjera i manevre, kontroleri brzine su elektronički moduli kojima se mjeri i upravlja brzinom leta. Vrlo je važno pred svaku letačku aktivnost provjeriti ispravnost i čvrsto prianjanje propelera za okvir i motor kako ne bi došlo do nesreća i neželjenih incidenata te na isto pripaziti kod njihove izmjene.

Zaštita propelera i motora – plastična kućišta u obliku kaveza namijenjena zaštiti fizičkog integriteta propelera i motora u slučaju kolizije bespilotne letjelice s vanjskim faktorom kako bi se spriječila djelomična ili potpuna oštećenja te u konačnici i sam pad bespilotnog zrakoplova. Ovaj element ovisi o modelu i proizvođaču te se često ne odlazi u osnovnom paketu komercijalnih bespilotnih zrakoplova već se smatra dodatnom opremom.

GNSS prijemnik – moduli koji omogućuju bespilotnom zrakoplovu komunikaciju sa satelitskim navigacijskim sustavima poput GPS-a (engl. *Global Positioning System*), GALILEO-a, GLONASS-a (rus. *Globalnaya Navigatsionnaya Sputnikovaya Sistema*) te BEIDUO-a. Omogućavaju satelitsko pozicioniranje, mjerenje letne visine, vizualizaciju letnog puta na karti, autonomnih letačkih funkcija te sigurnosnih funkcija poput tzv. „*return to home*“ vraćanja na uzletnu poziciju. Nije uključen u sve bespilotne zrakoplove, ovisno o namjeni.

Radio prijemnik – elektronički modul i antenski ustav zaslužan za prijem upravljačkih radio signala koji su odaslani sa zemaljske kontrolne postaje, bilo fiksne ili pak u obliku daljinskog upravljača, kontrolera.

Radio odašiljač – elektronički modul i antenski sustav, najčešće izveden u obliku daljinskoj upravljača pomoću kojeg operator tj. pilot na daljinu ručno zadaje naredbe koje se zatim odašilju do bespilotnog zrakoplova i u njemu obrađuju.

Pogonski izvor – najčešće u vidu praktičnih prijenosnih punjivih baterija u LiPo (engl. Lithium Polymer) izvedbi, malih dimenzija, prosječnog trajanja od 20 do 30 minuta.

Senzori – dodatni elektronički sklopovi, moduli ili posebni uređaji poput akcelerometra, inercijske mjerne jedinice (engl. *Inertial Measurement Unit* - IMU), senzor nagiba, magnetski senzor, strujni senzor te dodatna senzorska oprema poput akcijskih, termalnih ili kamera visoke razlučivosti u ovisnosti o potrebi krajnjeg korisnika tj. operatora na daljinu kao i senzori blizine za sprječavanje kolizije s objektima iz letne okoline , [9], [10], [11].

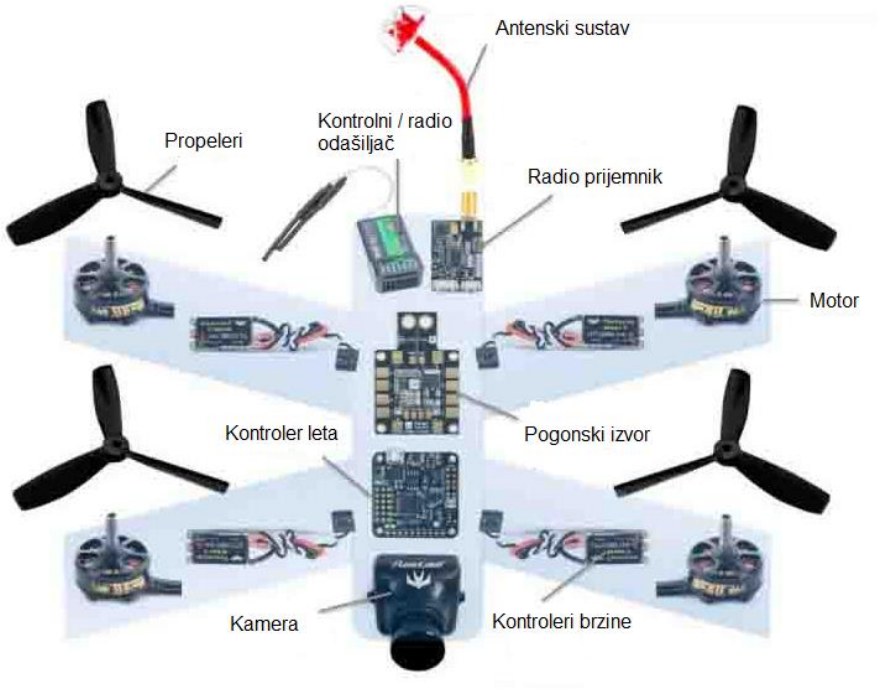
Akcelerometar pomaže odrediti poziciju tj. orijentaciju bespilotnog zrakoplova na način da mjeri ubrzanja pri manevrima. To su osjetljivi dijelovi koji mjere i najmanju promjenu sile potrebne za ubrzavanje koja se zatim uspoređuje s položajem u odnosu na utjecaj gravitacijskog polja.

Inercijska mjerna jedinica služi kod mjerenja smjera kretanja i nagiba u letu bespilotnog zrakoplova poput inercijskih podataka o ubrzanju, rotaciji i magnetnog polja duž svojih osi. Drugim riječima inercijska mjerna jedinica sastoji se od akcelerometra, žiroskopa i kompasa u izvedbi magnetometra.

Senzor nagiba služi kako bi bespilotan zrakoplov ostao u ravnini bez rizika od prevrtanja i pada dok za isto koristi kombinaciju žiroskopa i akcelerometra.

Magnetski senzor predstavlja izvedbu elektroničkog kompasa, vrlo bitnog kod mjerenja inercijskih veličina za navigaciju i pozicioniranje.

Strujni senzori upravljaju optimizacijom potrošnje energetskog izvora tj. baterije kako prema pojedinim pogonskim elementima tako i kontrolirajući strujne anomalije prouzročene kvarom neke komponente, pravovremeno obavještavajući pilota na daljinu o istom putem daljinskog upravljača ili povezanog pametnog mobilnog uređaja.



Slika 2. Dijelovi bespilotnog zrakoplova

Izvor: [12]

II. Programska podrška/softver

Svaki bespilotni zrakoplov treba softversku podršku za ostvarivanje letačkih operacija i ostalih funkcionalnosti. Ovisno o namjeni, rekreacijski i komercijalni bespilotni zrakoplovi na tržište dolaze s tvornički ugrađenim softverom u ovisnosti od samog proizvođača.

S druge strane tzv. DIY bespilotni zrakoplovi ovise o znanju i stručnosti osoba koje ga izrađuju, mogućnostima pojedinih komponenti i podržanim *open source* softverskim rješenjima.

Softversku komponentu bespilotnog zrakoplova i njene detalje, prema [13], [14], [15], [16] moguće je podijeliti u dvije kategorije:

a. Softver za upravljanje letom (engl. *Flight Management Software* - FMS)
b. Softver upravljačke zemaljske stanice (engl. *Ground Control Software* - GCS)

Softver za upravljanje letom (engl. *Flight Management Software* - FMS)

Namijenjen je osnovnom upravljanju bespilotnog zrakoplova prilikom uzlijetanja, manualnih i autonomnih letnih operacija te slijetanja uz dodatne funkcionalnosti poput stabilizacije i ručnog unosa navigacijskih parametara. Prethodno je instaliran kako s jedne strane u kontroler leta same letjelice tako s druge strane u daljinski upravljač putem kojeg se njome upravlja. Analogno ga možemo usporediti s Windows ili Android operativnim

sustavima za terminalne uređaje. Povezuje i omogućuje komunikaciju između kontrolera leta s ostalim komponentama bespilotnog zrakoplova.

Osim *proprietary* rješenja koja su tvornički implementirana u komercijalne ili rekreacijske bespilotne letjelice, postoji širok spektar raznih proizvođača trećih strana koji uz softversku podršku u obliku aplikacije za pametne mobilne uređaje pružaju dodatne mikrokontrolere za naknadnu ugradnju na bespilotan zrakoplov koji sadrže svu potrebnu logiku i senzoriku.

Važno je naglasiti kako je većina ovog tipa „operativnog“ softvera temeljena na jezgri Linux platforme poput Android OS-a. Neki od poznatijih su: Parrot AR Drone FC, Naza (DJI), Wookong (DJI), Dualsky (FC450) te *open source* Openpilot, Ardupilot (APM, Pixihawk), Multiwii te KKmultipcopter, [17].

Softver upravljačke zemaljske stanice (engl. *Ground Control Software* - GCS)

Koristi se kod upravljanja već preddefiniranih navigacijskih planova i rasporeda letnih operacija. Može sadržavati baze podataka ograničenih letnih zona te mehanizme za analizu i procesiranje kako telemetrije tako i ostalih senzorskih podataka. Izvodi se na uređajima poput računala ili pametnih mobilnih uređaja koji predstavljaju zemaljsku stanicu i to najčešće kad je sam bespilotni zrakoplov prizemljen te se za njega priprema plan puta tj. leta.

Neke od funkcionalnosti su mjerenja parametara s letjelice u stvarnom vremenu koja dodatno mogu biti vidljiva i ostalim sudionicima uključenih u letne operacije a ne samo operatoru, pilotu na daljinu. Osim njihove prezentacije, izmjerene vrijednosti mogu poslužiti kod prebacivanja u način rada autopilota. Kod komercijalnih bespilotnih zrakoplova izveden je kao letačka aplikacija.

2.2. Karakteristike bespilotnog zrakoplova DJI Mavic Air

U ovom diplomskom radu sav praktični dio istraživanja i analize bit će proveden na bespilotnom multikopter/multirotor zrakoplovu tvrtke DJI, točnije modelu Mavic Air. To je bespilotni zrakoplov za čije upravljanje se koristi kombinacija pripadajućeg daljinskog upravljača te pametnog mobilnog uređaja uz instaliranu DJI GO 4 letačku aplikaciju. Moguće je pojedinačno upravljanje daljinskim upravljačem (bez prijenosa slike u stvarnom vremenu) te pojedinačno upravljanje pametnim mobilnim uređajem (manji dolet).

DJI Mavic Air podržava korištenje posebnih letačkih naočala iz serije DJI Goggles FPV (engl. *First Person View*). Bespilotni zrakoplov se na pametni mobilni uređaj povezuje tzv. „*Enhanced Wi-Fi*“ tehnologijom koje se temelji na WLAN (engl. *Wireless Local Area Network*) 802.11 protokolu ali koristi veću razinu snage (dBm) u odašiljanju signala u oba smjera što omogućava veći domet signala te na kraju i veći dolet bespilotnog zrakoplova.

Kad se njime upravlja samo putem daljinskog upravljača, gube se dodatne funkcionalnosti poput pametnih, autonomnih režima leta i snimanja što nije slučaj pri povezivanju pametnog mobilnog uređaja tj. letačke aplikacije. Primjerak ovog bespilotnog zrakoplova koristi se za potrebe Laboratorija za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava, pri Zavodu za informacijsko-komunikacijski promet, [18].

Slika 3. Prikaz DJI Mavic Air bespilotnog zrakoplova, [19]

Iz tog razloga u nastavku slijedi tablični prikaz osnovnih tehničkih specifikacija vezanih za letne i ostale tehnološke mogućnosti bespilotnog zrakoplova DJI Mavic Air.

Tablica 1. Tehničke specifikacije DJI Mavic Air bespilotnog zrakoplova

Operativna masa (kod uzlijetanja):	430g
Dimenzije preklopljenog zrakoplova:	168*83*49mm (D*Š*V)
Dimenzije raskloplјenog zrakoplova:	168*184*64mm (D*Š*V)
Maksimalna brzina ulijetanja:	4m/s pri režimu leta Sport
Maksimalna brzina slijetanja:	3m/s pri režimu leta Sport
Maksimalna brzina leta (bez vjetra uz razinu mora):	68,4km/h ili 9 m/s pri režimu leta Sport
Maksimalna visina leta:	5000m
Maksimalno trajanje leta (bez vjetra):	21 min. (pri brzini od 25 km/h ili 6,9 m/s)
Maksimalna letna udaljenost/doseg:	10km
Maksimalna otpornost na brzine vjetra:	29-38km/h ili 8,05-10,5m/s
Operativna frekvencija letjelice i daljinskog upravljača:	F1: 2,400-2,4835 te F2: 5,725-5,850 GHz

Podržane GNSS tehnologije:	GPS+GLONASS
Unutarnja memorijska pohrana:	8GB
Podržani format SD memorijskih kartica:	microSD Class 10 ili UHS-1 na više (do 128GB)
Senzori blizine, položaj i osjetljivost:	Svjetlosni (prednji, stražnji i donji) uz LUX > 15
Maksimalna udaljenost odašiljanja s daljinskog upravljača (bez interferencija):	F1: 2000-4000m F2: 500-4000m
Kapacitet baterije daljinskog upravljača / baterije bespilotnog zrakoplova:	2970mAh / 2375mAh (LiPo 3S)
Podržane dimenzije daljinskog upravljača za pametni mobilni uređaj:	Maksimalna dužina: 160mm Podržana debljina: 6,5-8,5mm
Podržani USB priključci daljinskog upravljača:	Lightning, Micro USB (Tip-B), USB-C
Stabilizacijski okvir kamere/*Gimbal*:	3-osni (nagib, rotacija, pomak)
Kamera (senzor/leća):	1/2,3“CMOS uz 12 MP / f/2,8 uz širinu 85°
Rezolucija fotografija:	4:3 format = 4056x3040p 16:9 format = 4056x2280p
Rezolucija videozapisa:	4K Ultra HD: 3840×2160 24/25/30p 2.7K: 2720×1530 24/25/30/48/50/60p FHD: 1920×1080 24/25/30/48/50/60/120p HD: 1280×720 24/25/30/48/50/60/120p *Live* prijenos na mem. pametnog mobilnog uređaja: 720p@30fps
Podržani format datotečnog sustava:	FAT32
Podržani format fotografija / videozapisa:	JPEG/DNG(RAW) / MP4/MOV (H.264/MPEG-4 AVC)
Potrebna letačka aplikacija i sustav video prijenosa:	DJI GO 4 (*Enhanced Wi-Fi*)
Latencija prijenosa (ovisno o uvjetima):	170-240ms

Izvor: [18]

2.3. Potencijalni izvori podataka prema elementima ekosustava bespilotnih zrakoplova

Kod forenzičke analize bespilotnih zrakoplova vrlo je važno znati gdje tražiti određene podatke koji bi se kasnije mogli iskoristiti u nekoj parnici. Prvo i osnovno, što većina ljudi smatra je ekstrakcija video materijala s unutarnje ili vanjske pohrane, što je naravno točno jer takav video materijal može primjerice sadržavati dodatne informacije iz snimljene okoline koje bi mogle biti važne za slučaj (automobilske registracije, ljude iz okoline i njihova kretanja, vrijeme i sl.).

Također je bitno ekstrahirati podatke koje mogu dodatno obogati glavni video dokaz, a takve podatke obično kreiraju senzori samog drona, daljinski upravljači/kontroleri te letačke aplikacije tj. svi ostali sekundarni elementi, [20].

Na bespilotni zrakoplov potrebno je gledati kao na pametni terminalni uređaj koji svakim svojim korištenjem, nekim načinom povezivanja i ostalog, kreira nove digitalne dokaze, bilo izravnom namjerom krajnjeg korisnika ili tvorničkim postavkama.

U nastavku slijedi popis potencijalnih tipova podataka koji su generirani u povezanim elementima sustava bespilotne letjelice:

a. Multimedijski tj. audio-video podaci
b. Podaci kreirani povezanom dodatnom nosećom opremom
c. Plan i raspored letnih operacija
d. *Log* podaci o korištenju bespilotnog zrakoplova

<u>Multimedijski tj. audio-video podaci</u>

Oni predstavljaju najveći volumen podataka prema njihovoj veličini (zauzeće memorijskog prostora), kreiranih kamerama visoke razlučivosti, te je njihovo dohvaćanje jedan od prvih motiva forenzičke analize bespilotnih letjelica. Kod rekreacijskih i komercijalnih bespilotnih letjelica isti su u obliku kvalitetnih fotografija i videozapisa pohranjenim na vanjsku ili unutarnju memoriju bespilotnog zrakoplova. Upravo ova značajka, marketinški je vrlo primamljiva krajnjim korisnicima.

<u>Podaci kreirani povezanom dodatnom nosećom opremom</u>

Tu spadaju razni namjenski uređaji i pomoćna oprema kad se bespilotni zrakoplovi koriste za točno određenu namjenu. Primjerice oprema za podizanje/spuštanje/dostavu tereta, termo-vizijski senzori i kamere i sl. Oni generiraju različite tipove podataka koji su pripremljeni za prikaz operatoru ili drugim osobama, a kao takvi mogu biti: vrijeme i datum aktivnosti, detalji izvršenih zadataka u aktivnosti, osvrt na letne operacije i sl.

Plan i raspored letnih operacija

Određeni bespilotni zrakoplovi posjeduju značaju autonomnog ili poluautonomnog leta. On se ostvaruje unaprijed zadanim instrukcijama i naredbama operatora ili rasporedom budućih aktivnosti. Prilikom takvih letačkih operacija, bespilotni zrakoplov putem mreže senzora prikuplja podatke i distribuira ih na kontrolnu stanicu putem koje operator može pratiti njemu bitne podatke o trenutnom stanju leta i izvođenju operacija.

Ti podaci vrlo često ostaju dostupni za pregled na kontrolnoj stanici nakon završetka leta. Putem letačkih aplikacija ili sličnih namjenskih softvera ti podaci mogu biti povezani i prikazani na karti što pruža bogatiji set informacija.

Log podaci o korištenju bespilotnog zrakoplova

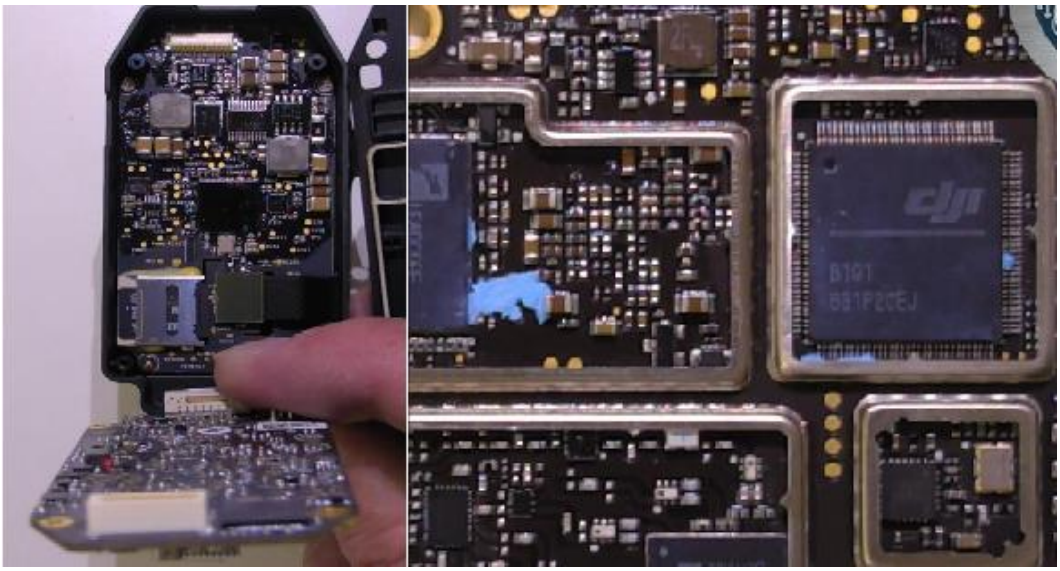
Svaka interakcija vezana uz bespilotni zrakoplov i njegovu osnovnu letnu opremu generira određeni skup podataka tj. metapodataka analogno s korištenjem pametnim mobilnih terminalnih uređaja. Često ta skupina podataka nije zamišljena na način da se prikazuje krajnjem korisniku te da pruži dodatne informacije. Primjer takvih podataka su: vrijem i datum aktivnosti određene funkcije, lokacije točaka na letnom putu, navigacijski parametri, brzina, visina i pravac kretanja itd.

Što se tiče pristupa konkretnim tipovima podataka na pojedinim elementima bespilotne letjelice, isti ovisi prvenstveno o samom proizvođaču, danim tehničkim specifikacijama, konfiguraciji bespilotnog zrakoplova prema želji i potrebi operatora. U praksi to može značiti dohvaćanje zanemarivog ili pak velikog i kompleksnog seta podataka.

Iz tog razloga treba uzeti u obzir ljudski faktor korištenja osim same tehničke značajke bespilotne letjelice te nakon apsolviranja istog puno je lakše pristupiti ključnim mjestima u smislu forenzičke ekstrakcije.

Slijedi popis nekoliko lokacija, prema [21], unutar kojih je moguće pronaći kritične podatke tijekom istrage:

a. Unutarnja memorijska pohrana
b. Vanjska izmjenjiva memorijska pohrana
c. Daljinski upravljači
d. Pametni mobilni uređaji
e. Zemaljske stanice
f. Podatkovne platforme temeljene na *cloud* usluzi



Slika 4. Prikaz unutarnje pohrane na kontroleru leta DJI bespilotnog zrakoplova

Izvor: [22]

Unutarnja memorijska pohrana

Samo određeni bespilotni zrakoplovi imaju kapacitet za unutarnju pohranu koja se nalazi unutar okvira ili na kontroleru u izvedbi umetnute memorijske kartice ili u izvedbi eMMC (engl. *Embedded Multi-Media Controller*) čipa. Njihov kapacitet varira od modela i proizvođača.

Ovisno o modelu, dohvat njihovog sadržaja može biti jednostavan na principu „*plug and play*“ ili je pak potrebna neka od invazivnijih metoda ekstrakcije poput *chip-off* metode. Obično sadrže multimedijske, foto te video podatke ali i *log* zapise letova. Oni se mogu sastojati od putanja leta, uzletnih i sletnih koordinata, ID kontrolera, podataka o operatoru i sl.

Vanjska izmjenjiva memorijska pohrana

Jedan od najčešće korištenih standarda kod vanjske memorije bespilotnih zrakoplova je *microSD* kartica. Određeni modeli bespilotnih zrakoplova posjeduju mogućnost pohranjivanja isključivo na istu, koja ne mora nužno doći u osnovnom pakiranju.

Uzimajući u obzir njene male dimenzije koje štede prostor, veliki memorijski kapacitet i nisku cijenu razumljiva je njena široka uporaba u području bespilotnih letjelica. Također, kao i unutarnji tip pohrane prvenstveno sadrži multimedijske podatke ali i ostale prethodno opisane.

Daljinski upravljači

Određeni modeli bespilotnih letjelica zahtijevaju korištenje daljinskog upravljača za njihovo upravljanje dok drugi isto omogućuju i putem pametnog mobilnog uređaja. Daljinski upravljač može sadržavati podatke ključne za identifikaciju bespilotnog zrakoplova s kojim je povezan i uparen, a ukoliko se koristi uz kombinaciju s pametnim mobilnim uređajem može poslužiti i za njegovu identifikaciju (a zatim i pilota na daljinu).

Na daljinskom upravljaču moguće je također pronaći *log* zapise leta (ovisno o modelu i proizvođaču) te podatke o povezanim uređajima i neke metapodatke poput: serijski broj drona, inačica *firmware*-a, tzv. *home* sletne točke, Wi-Fi, SSID (engl. *Service Set Identifier*), MAC (engl. *Media Access Control*), IP (engl. *Internet Protocol*) te Bluetooth informacije o povezanom dronu i mobilnom terminalnom uređaju ili uređajima.

Pametni mobilni uređaji

Upravljanje bespilotnim zrakoplovom ili njegovom dodatnom opremom moguće je provesti putem njima povezanih pametnih mobilnih uređaja kroz pripadajuću letnu/upravljačku aplikaciju.

Na samim pametnim mobilnim uređajima moguće je analizirati podatke generirane kroz letačku aplikaciju koja većinom kombinira podatke koji su prethodno opisani (uz dodatne informacije o MAC, IMEI – engl. *International Mobile Equipment Identity*, i IMSI – engl. *International Mobile Subscriber Identity* broju uređaja te podatke korisnika o prijavi putem Google-a, Facebook-a, inačicu mobilnog operativnog sustava i sl.).

Zemaljske stanice

Tu spadaju stanice za kontrolu bespilotnog zrakoplova sa zemlje s mogućnostima poput planiranja rute i letnih operacija, FPV letačkih naočala, promatranja unutar vidnog polja ili prijenos u stvarnom vremenu s kamere bespilotnog zrakoplova na medij lokalne pohrane. Obično se dohvaćanje tog tipa podataka vrši kroz analizu namjenskih aplikacijskih rješenja tih zemaljskih stanica ili analizom samih stanica kroz sofisticirane forenzičke alate.

Podatkovne platforme temeljene na *cloud* usluzi

U njih se ubrajaju *cloud* usluge trećih strana ili rješenja proizvođača bespilotne letjelice. Takve platforme mogu sadržavati razne multimedijske i ostale podatke povezane s letačkom aplikacijom koji se manualno ili automatizirano prebacuju na neki od tih servisa.

Podaci s *cloud* pohrane te s letačkih naočala mogu pružiti dodatno obogaćivanje već prikupljenih sadržaja jer se u njihovom slučaju radi o većim količinama, npr. prethodni letni sadržaj i metapodaci koji su uklonjeni, obrisani s drona ili daljinskog upravljača zbog primjerice potrebe oslobađanja prostora lokalne pohrane, [20], [21], [22], [23].

Važno je istaknuti kako različiti proizvođači dronova koriste različite, što *open-source* što vlastite operativne sustave u samim letjelicama, stoga i način pohrane senzorskih podataka, *log* zapisa o letu te na kraju i multimedijskih podataka nije identičan što se pak odražava na formate datoteka. Primjerice određeni dronovi proizvođača Yunecc tvornički spremaju *log* zapise letenja kao format .CSV, proizvođač DJI kao format .DAT i .TXT a proizvođač 3DR kao .LOG datoteke.

Također, prilikom akvizicije podataka s mobilne aplikacije i terminalnog uređaja, istražitelj bi trebao provjeriti postoji li još koja letačka aplikacija trećih strana instalirana na mobilnom terminalnom uređaju te ako postoji, je li bila korištena i forenzički kompromitirana. Ako je korištena, ona tada isto postaje izvor dokaza kojeg se mora pregledati i ekstrahirati, [24].

3. Regulatorni aspekt primjene bespilotnih zrakoplova u RH

Prvenstveno govoreći vrlo je važno odrediti regulatorne standarde kojih se piloti bespilotnih zrakoplova moraju pridržavati kod izvođenja letačkih operacija kako ne bi doveli u pitanje sigurnost drugih ljudi, imovine te općenito njihove operativne okoline. S obzirom na činjenicu kako je primjena bespilotnih zrakoplova u opće društvene svrhe relativno raširena, zakonodavna tijela nisu svugdje prepoznala potrebu donošenja pravnog okvira njihovog korištenja.

S popularizacijom korištenja te padom cijena dronova za komercijalnu i civilnu upotrebu pokazivat će se sve veća potreba za regulacijom tog područja kao i za donošenjem zakonodavnih okvira u provođenju ispitivanja takvih letjelica kroz postupke i metodologije digitalne forenzike. Kako bi postojala potreba za provedbom postupaka digitalne forenzike nad dronovima u sudske svrhe, pretpostavka je da je određeni pilot koristio letjelicu na nezakonite načine te tako ugrozio sigurnost sebe i svoje okoline bilo na fizički način ili narušavanjem privatnosti.

U većini zemalja letačke operacije regulirane su od strane civilnih agencija, dok su prema podacima Interpola zemlje poput Alžira, Barbadosa, Bruneja, Obale Bjelokosti, Kube, Irana, Kuvajta, Kirgistana, Madagaskara, Maroka, Nikaragve, Saudijske Arabije, Senegala te Sirije u potpunosti zabranile korištenje bespilotnih zrakoplova u civilne i privatne svrhe.

3.1. Zakonski okvir operativne primjene bespilotnih zrakoplova u RH

Što se tiče Republike Hrvatske, za regulaciju operativnih civilnih letačkih radnji zadužena je hrvatska agencija za civilno zrakoplovstvo (CCAA) te surađuje s krovnom europskom agencijom za sigurnost civilnog zrakoplovstva – EASA-om (engl. *European Union Aviation Safety Agency*).

U Republici Hrvatskoj prije svakog leta, isti je potrebno prijaviti putem web obrasca CCAA ako operativna masa bespilotnog zrakoplova prelazi 900 grama te je također maksimalna dopuštena visina leta 120 metara iznad razine tla ili do 50 metara iznad prepreke, ovisno što je više. Također su određene i regulirane kategorije bespilotnih zrakoplova koje će biti prikazane uz važne karakteristike kao što su: dob operatora izvođenja letačkih aktivnosti te položen teorijski ispit određenih zrakoplovnih propisa.

Zakonodavni aspekt operativnog letenja opisuje *Pravilnik o sustavima bespilotnih zrakoplova* (NN 104/2018), [25], donesen od strane Ministarstva pomorstva, prometa i infrastrukture koji kroz svojih 17. članaka određuje obavezne oznake dronova, pravila letenja, dužnosti i obaveze pilota na daljinu, kategorizaciju i pravo izvođenja letačkih operacija, potrebnu letnu dokumentaciju i ostalo. Jedna od važniji stavka jest zabrana izravnog letenja u blizini ljudi na manjoj horizontalnoj udaljenosti od 30 metara.

Tablica 2. Kategorizacija bespilotnih letjelica u RH

Kategorija letačkih operacija		A	B1	B2	C1	C2
Bespilotni zrakoplov	Operativna masa bespilotnog zrakoplova	OM<250g	250g<=OM<=900g	OM<5kg	5kg<=OM<=25kg	5kg<=OM<=150kg
	Najveća brzina bespilotnog zrakoplova prema tehničkim specifikacijama proizvođača	< 19 m/s	< 19 m/s	Nije primjenjivo	Nije primjenjivo	Nije primjenjivo
Izvođenje letačkih operacija	Dio dana	Danju i/ili noću	Danju	Danju i/ili noću	Danju	Danju i/ili noću
	Područje izvođenja operacija	Naseljeno i/ili nenaseljeno	Nenaseljeno	Naseljeno i/ili nenaseljeno	Nenaseljeno	Naseljeno i/ili nenaseljeno
Zahtjevi za pilota na daljinu	Minimalna dob	Nije propisano	14 god. ili manje od 14. god. Pod nadzorom punoljetne osobe	16. god.	18. god.	18. god.
	Polaganje teorijskog/praktičnog ispita	Nije potrebno	Nije potrebno	Nije potrebno	Položen teorijski ispit iz poznavanja primjenjivih zrakoplovnih propisa	**a)**Položen teorijski ispit iz poznavanja primjenjivih zrakoplovnih propisa **b)**Demonstracija pripreme leta i letenja
Zahtjevi za operatora	Obaveza evidentiranja/odobrenja operatora	Nije potrebno	Nije potrebno	Potrebna evidencija	Potrebna evidencija	Potrebno odobrenje – obratiti se HACZ
	Dokumentacija operatora	Nije potrebno	Nije potrebno	Nije potrebno	Nije potrebno	**a)** Operativni priručnik **b)** Zapisi o letu **c)** Upravljanje rizicima

Izvor: [26], [27]

Prije bilo kakvih aktivnosti važno je odrediti pripadnost bespilotnog zrakoplova jednoj od kategorija vidljivih iz prethodne tablice. Najčešće se za utvrđivanje same kategorizacije letjelica koriste njene dvije tehničke karakteristike već prethodno spomenute:

I. Operativna masa bespilotnog zrakoplova tj. ukupna masa bespilotnog zrakoplova u trenutku uzlijetanja
II. Najveća dopuštena brzina bespilotnog zrakoplova (tvornički određena)

Prije pristupa samim letačkim operacijama, prema *Pravilnik o sustavima bespilotnih zrakoplova* (NN 104/2018), [25], potrebno je izvršiti označavanje bespilotnog zrakoplova na sljedeći način:

I. Označavanje identifikacijskom negorivom pločicom
II. Označavanje identifikacijskom naljepnicom (za bespilotne zrakoplove operativne mase do 5 kg)
III. Identifikacijska pločica ili naljepnica mora sadržavati:
    - Ime, adresu, kontakt podatke operatora ili vlasnika
    - Jedinstvenu identifikacijsku oznaku bespilotnog zrakoplova (za kategoriju C2) koju dodjeljuje Hrvatska agencija za civilno zrakoplovstvo
IV. Identifikacijska pločica ili naljepnica mora biti odgovarajuće veličine koja omogućuje jasnu identifikaciju podataka na istoj

Prethodno navedeno znači kako bespilotni zrakoplov DJI Mavic Air spada u kategoriju B1 što zbog svoje operativne mase te maksimalne brzine leta. Isti može letjeti i manjim brzinama od one navedene u tablici, ovisno koju način leta je odabran kroz letačku aplikaciju.

Također, vršenje letačkih operacija ovim modelom bespilotnog zrakoplova, prema zakonu moguće je isključivo danju u nenaseljenom području. Minimalno dobna granica za pilota na daljinu je 14. godina dok njegova evidencija te evidencija samog zrakoplova kod regulatora tj. Hrvatske agencije za civilno zrakoplovstvo nije potrebna.

Što se pravila letenja tiče, ona se odnose na sljedeće:

I. Bespilotnim zrakoplovom dopušteno je letenje:
    - u nekontroliranom zračnom prostoru na visini do 120 m iznad razine tla ili do 50 m iznad prepreke, ovisno što je više
    - u kontroliranom zračnom prostoru izvan prostora polumjera 5 km od referentne točke aerodroma na visini do 50 m iznad razine tla
    - a udaljenosti od najmanje 3 km od rubova i pragova uzletno-sletne staze (USS) nekontroliranog aerodroma

- na način da horizontalna udaljenost bespilotnog zrakoplova od skupine ljudi nije manja od 50 m, osim kada se bespilotnim zrakoplovom sudjeluje na zrakoplovnoj priredbi
- na način da horizontalna udaljenost od ljudi koji nisu uključeni u operacije nije manja od visine leta i nije manja od 5 m kada je na bespilotnom zrakoplovu uključen način rada na maloj brzini i kada je najveća dopuštena brzina podešena na 3 m/s, ili 30 m u ostalim slučajevima
- unutar vidnog polja pilota na daljinu
- uz uspostavu *ad hoc* strukture u skladu s primjenjivim propisom o upravljanju zračnim prostorom

II. <u>Kada se bespilotni zrakoplov koristi za potrebe rekreacije i sporta dopušteno je:</u>
- izvođenje leta koristeći prikaz pogleda iz bespilotnog zrakoplova (engl. FPV – *first person view*)
- letenje samo u nenaseljenom području i iznimno letenje na visini većoj od 120 m iznad tla

III. <u>Bespilotnim zrakoplovom nije dopušteno:</u>
- prevoziti opasnu robu, teret, ljude i životinje
- izbacivanje predmeta tijekom leta
- letenje iznad skupine ljudi

Za navedeni model bespilotnog zrakoplova prethodno bi značilo kako je njime dopušteno letenje do maksimalne visine koja iznosi 120 metara iznad razine tla ili 50 maksimalno 50 metara ispred određene prepreke na koju se naiđe tijekom leta poput stabala, planina, kuća, zgrada i sl. Također je zabranjeno ulaženje u zonu od 3 km od rubova aerodroma zbog same sigurnosti odvijanja prometa, zrakoplovnog osoblja, putnika i infrastrukture.

Najmanja horizontalna udaljenost od ljudi u letnoj okolini mora biti 50 metara dok je visina leta iznad manje grupe ljudi minimalno 5 metara. Horizontalna udaljenost se može smanjiti na 30 m od ljudi ako se brzina leta bespilotnog zrakoplova ograniči određenim režimom letenja na 3 m/s. Let je dozvoljen samo do dometa vidnog polja operatora, što ponajviše ovisi o okruženju u kojem isti izvodi letne operacije (ruralno ili urbano područje, prepreke na području ili čistina i sl.). Izrazito se zabranjuje let iznad veće skupine ljudi kao i prijevoz robe, tereta na bespilotnom zrakoplovu kao i izbacivanje predmeta s njega tijekom leta.

Sama masa DJI Mavic Air bespilotnog zrakoplova, kao i njegove dimenzije ne dopuštaju tzv. „uradi sam“ projekte kojima bi se potencijalno neki predmeti mogli na istog učvrstiti i to sve iz razloga što bi u tom slučaju bile kompromitirane letne karakteristike i sama nosivost (dostatan za vlastitu masu).

Nadalje, pravilnik određuje dužnosti i odgovornosti pilota na daljinu:

I. Pilot na daljinu mora:
   - upravljati bespilotnim zrakoplovom na siguran način, da ne predstavlja opasnost po život, zdravlje ili imovinu na tlu i u zraku te da ne narušava javni red i mir
   - upravljati bespilotnim zrakoplovom sukladno primjenjivim propisima, letačkom priručniku ili uputama za upotrebu i operativnom priručniku kada je primjenjivo
   - prije leta provjeriti ispravnost sustava bespilotnog zrakoplova
   - provjeriti da li je bespilotni zrakoplov označen u skladu s ovim propisom
   - osigurati područje uzlijetanja i slijetanja
   - prikupiti sve potrebne informacije za planirani let i uvjeriti se da meteorološki i ostali uvjeti u području leta osiguravaju sigurno izvođenje leta
   - osigurati da je sva oprema ili teret na bespilotnom zrakoplovu odgovarajuće pričvršćen na način da ne dođe do njegovog ispadanja
   - upravljati na način da bespilotni zrakoplov tijekom uzlijetanja ili slijetanja sigurno nadvisuje sve prepreke
   - stalno promatrati zračni prostor u području letenja bespilotnog zrakoplova kako ne bi doveo u opasnost druge zrakoplove
   - dati prednost zrakoplovu s posadom

II. Pilot na daljinu ne smije upravljati:
   - istovremeno s više bespilotnih zrakoplova i/ili
   - unutar područja gdje se izvodi hitna intervencija

Dužnosti i odgovornosti pilota na daljinu pružaju smjernica kojih se treba držati kako bi se osigurala sigurnost svih sudionika letačkih operacija, ljudi izvan nje pa tako i objekata, stvar i životinja iz njene okoline.

Unutar propisa, *Pravilnik o sustavima bespilotnih zrakoplova* (NN 104/2018), [25], navedene su određene mjere koje odstupaju od ovdje prethodno navedenih pravila te je za let izvan njih operator na daljinu dužan ishoditi odobrenje Hrvatske agencije za civilno zrakoplovstvo.

Kako to mogu biti izrazite i specifične situacije (npr. let na visini većoj od 120 metara i sl.), iste u ovom dokumentu nisu opisane. Članci i točke ovog pravilnika koje se još odnose na:

a) Opremu bespilotnog zrakoplova za izvođenje letačkih operacija noću
b) Zapise o letu
c) Upravljanje rizicima
d) Operativni priručnik
e) Evidenciju operatora
f) Odobrenja Agencije
g) Obaveznu dokumentaciju

Također, isti nisu opisani u ovom radu jer se odnose na bespilotne zrakoplove viših kategorija (tablica 2.) te iste nije potrebno posjedovati i primjenjivati kod malih bespilotnih zrakoplova kategorija B i B1 unutar koje spada i DJI Mavic Air.

3.2. Zakonski okvir pri aktivnostima snimanja iz zraka u RH

Ako se govori o ostalim aktivnosti tijekom letnih operacija tj. o posebnim operacijama radova iz zraka, najčešće se tu podrazumijeva snimanje ili fotografiranje. Prema samoj izvedbi današnjih civilnih bespilotnih zrakoplova koji mogu i najčešće na sebi sadrže potrebnu opremu u obliku akcijskih kamera visoke razlučivosti.

Takve aktivnosti mogu ugroziti privatnost ljudi i državne sigurnosti u okolini leta bespilotnih zrakoplova te su iste uređene *Uredbom o snimanju iz zraka* (NN 28/2019), [28]. U uredbi je definirano kako je snimanje iz zraka posebna operacija radova nad teritorijem Republike Hrvatske kod koje se uređaj za snimanje nalazi na ili u zrakoplovu ali se ističe da se uredba ne odnosi na snimanja bespilotnim letjelicama za osobne svrhe osim ako nije riječ o tzv. *ciljanom snimanju* koje obuhvaća sljedeće stavke članka 4. ove uredbe:

(1) Ciljano snimanje iz zraka vojnih i civilnih lokacija i građevina posebno važnih za obranu obavlja se na temelju suglasnosti vlasnika, odnosno korisnika.

(2) Ciljano snimanje iz zraka industrijske lokacije i građevine za potrebe vlasnika, odnosno korisnika koje se obavlja u svrhu praćenja stanja izgrađenosti, oštećenosti odnosno zaštite, može se obaviti sustavima bespilotnih zrakoplova u skladu s propisima o sustavima bespilotnih zrakoplova, bez odobrenja Državne geodetske uprave za snimanje iz zraka.

(3) Ciljano snimanje iz zraka koje provodi tijelo nadležno za obavljanje inspekcijskih poslova u području građenja može se obaviti sustavima bespilotnih zrakoplova u skladu s propisima o sustavima bespilotnih zrakoplova bez odobrenja Državne geodetske uprave za snimanje iz zraka.

(4) Snimljeni materijal koji nastane ciljanim snimanjem iz stavaka 2. i 3. ovoga članka može se koristiti za interne potrebe vlasnika, odnosno korisnika, a za njegovo javno objavljivanje podnosi se zahtjev Državnoj geodetskoj upravi.

(5) Ciljano snimanje iz zraka je i snimanje za potrebe izvještavanja o kulturnim i sportskim priredbama/manifestacijama te izvanrednim događajima, kao što su prometne gužve, prometne nesreće, prirodne nepogode (poplave, požari, potresi i sl.), koje smiju snimati isključivo televizijske kuće s nacionalnom koncesijom te pravne ili fizičke osobe koje obavljaju snimanja za njih, na temelju izdanog odobrenja za snimanje iz zraka u kojem slučaju se iznimno pribavlja jedno odobrenje za snimanje iz zraka.

(6) Snimke iz stavka 5. ovoga članka mogu se iznimno koristiti bez prethodnog pregleda Državne geodetske uprave isključivo radi prijenosa uživo i izvještavanja javnosti, a snimljeni materijal dostavlja se na pregled naknadno u Državnu geodetsku upravu odmah po obavljenom snimanju, a najkasnije u roku od osam dana od završetka snimanja.

(7) Operator snimanja koji upravlja bespilotnim zrakoplovom dužan je prilikom obavljanja ciljanog snimanja pridržavati se odredaba propisa koji uređuju zaštitu osobnih podataka.

Ako je riječ o tzv. *Ciljanom snimanju* iz zraka, operator letenja / operator snimanja dužan je zatražiti odobrenje[1] za snimanje iz zraka i uporabu zračnih snimki od Državne geodetske uprave.

Uz zahtjev, među ostalim dokumentima, potrebno je priložiti i potvrdu o uplati upravne pristojbe u iznosu od 15 HRK za odobrenje za snimanje iz zraka te dodatnih 15 HRK za odobrenje za uporabu zračnih snimaka. Taj zahtjev mora sadržavati sljedeće podatke (članak 5.):

(1) Zahtjev za odobrenje za snimanje iz zraka i uporabu zračnih snimaka podnosi se Državnoj geodetskoj upravi i mora sadržavati sljedeće podatke:
- podatke o naručitelju snimanja (naziv, adresa sjedišta i OIB)
- podatke o snimatelju (naziv, adresa sjedišta i OIB) i dokaz o registriranoj djelatnosti snimanja iz zraka izdanog od strane nadležnog tijela u Republici Hrvatskoj, odnosno nadležnog inozemnog tijela. Dokaz o registriranoj djelatnosti inozemnog snimatelja prilaže se u ovjerenom prijevodu na hrvatski jezik
- podatke o operatoru snimanja (ime, prezime, adresa, zanimanje i OIB)
- podatke o zrakoplovu (proizvođač, tip/model, registracijska oznaka ako je primjenjivo)

[1] **Izdavanje odobrenja za snimanje iz zraka i uporabu zračnih snimaka**. Preuzeto sa: https://gov.hr/moja-uprava/aktivno-gradjanstvo-i-slobodno-vrijeme/sport-i-rekreacija/izdavanje-odobrenja-za-snimanje-iz-zraka-i-uporabu-zracnih-snimaka/1962

- podatke o operatoru zrakoplova (naziv, adresa sjedišta, OIB, osoba za kontakt, telefon, fax, e-mail)
- podatke o vremenskom razdoblju snimanja (dan, mjesec, godina)
- svrhu snimanja (izmjera zemljišta, istraživanje, prostorno uređenje te druge gospodarstvene i znanstvene potrebe)
- plan snimanja na karti u prikladnom mjerilu s označenim područjem snimanja, izuzev za bespilotne zrakoplove koji snimaju do radijusa 500 m od centra snimanja
- podatak radi li se o ciljanom snimanju (priložiti popis lokacija i građevina)
- podatke o vrsti snimanja (analogno/digitalno), MS/GSD, kameri/senzoru, žarišnoj daljini objektiva, obliku zapisa (film ili format digitalnog zapisa snimke)

(2) Za snimanje područja zaštićenih dijelova prirode, pored podataka navedenih u stavku 1. ovoga članka, dostavlja se suglasnost javne ustanove koja je nadležna za upravljanjem tim područjem.

(3) Zahtjev za odobrenje za snimanje iz zraka i uporabu zračnih snimaka podnosi naručitelj snimanja, odnosno pravna ili fizička osoba po ovlasti naručitelja snimanja.

Iz prethodnih stavka vidljivo je kako za provođenje letačkih aktivnosti potrebna dozvola Hrvatske agencije za civilno zrakoplovstvo dok je za snimanje i korištenje snimljenog materijala potrebna dozvola Državne geodetske uprave ili od Ministarstva obrane za strane državljane ukoliko je riječ o kategoriziranom *ciljanom snimanju*.

Kada je riječ o tzv. hobističkom, rekreativno snimanju za osobne svrhe koje ne ulazi u kategorizirano *ciljano* snimanje iz zraka, isto nije potrebno prijaviti niti snimljeni materijal dostaviti Državnoj geodetskoj upravi na pregled (dopuštenje o objavi snimaka).

Postoji mala nelogičnost u cijelom procesu jer kod zahtjeva za odobrenje za snimanje iz zraka i uporabu zračnih snimki treba navesti podatak radi li se o *ciljanom snimanju* što bi odmah trebalo biti jasno jer je zahtjev potrebno podnesi isključivo ako je riječ o *ciljanom snimanju*.

Također vrlo je važno napomenuti kako su operatori tj. piloti na daljinu obvezani poštovati Ispravak Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) tzv. **GDPR**-a (engl. *General Data Protection Regulation*).[2]

[2] **UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)**. Preuzeto sa: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679

Za navedeno ne postoje strogo definirana pravila kojima se ono provodi tj. na koji način se smije snimati bespilotnim zrakoplovom a da se pritom ne narušava pravo na privatnost pojedinca. Kako stoji u izvoru [29], rekreativni korisnik bespilotnih zrakoplova treba obrati pažnju na sljedeće:

a) Vaša aktivnost za privatnost drugih ljudi potencijalno je invazivna te se na vas može primijeniti zakonodavstvo za zaštitu podataka
b) Sve dok je vaš bespilotni zrakoplov opremljen kamerom, snimačem videozapisa ili bilo kojim uređajem kojim se mogu snimiti osobni podaci uključujući slike, razgovore, lokaciju itd., primjenjuje se zakonodavstvo za zaštitu privatnosti
c) Bespilotne zrakoplove uvijek morate odgovorno upotrebljavati te ne ometati privatnost drugih ljudi
d) Nemojte snimati fotografije, videozapise ili zvučne zapise ljudi u njihovom domu, vrtu, autu itd., bez njihove dozvole
e) Zaštita podataka i privatnost primjenjuje čak i na javnim mjestima. U određenim okolnostima i imovina ljudi može biti zaštićena
f) Postoji opasnost da rad vašeg bespilotnog zrakoplova predstavlja napad na privatnost čak i ako on nije opremljen kamerom ili drugim senzorima

Također neke opće preporuke za smanjenje mogućih incidenata kod snimanja iz zraka i potencijalnog narušavanja uredbe o zaštiti i privatnosti osobnih podataka su:

- Poštujte pravo na privatnost – ne koristite bespilotni zrakoplov za namjerno narušavanje privatnosti drugih ljudi
- Kad je god moguće obavijestite ljude iz okoline o svojim namjerama i budućem snimanju iz zraka te ih pitajte za dopuštenje ako će istim biti obuhvaćeni
- Važno je razmisliti i uzeti u obzir činjenicu da prilikom objave snimaka na Internetu ili društvenim mrežama možda potencijalno ugrožavate nečije osobne podatke

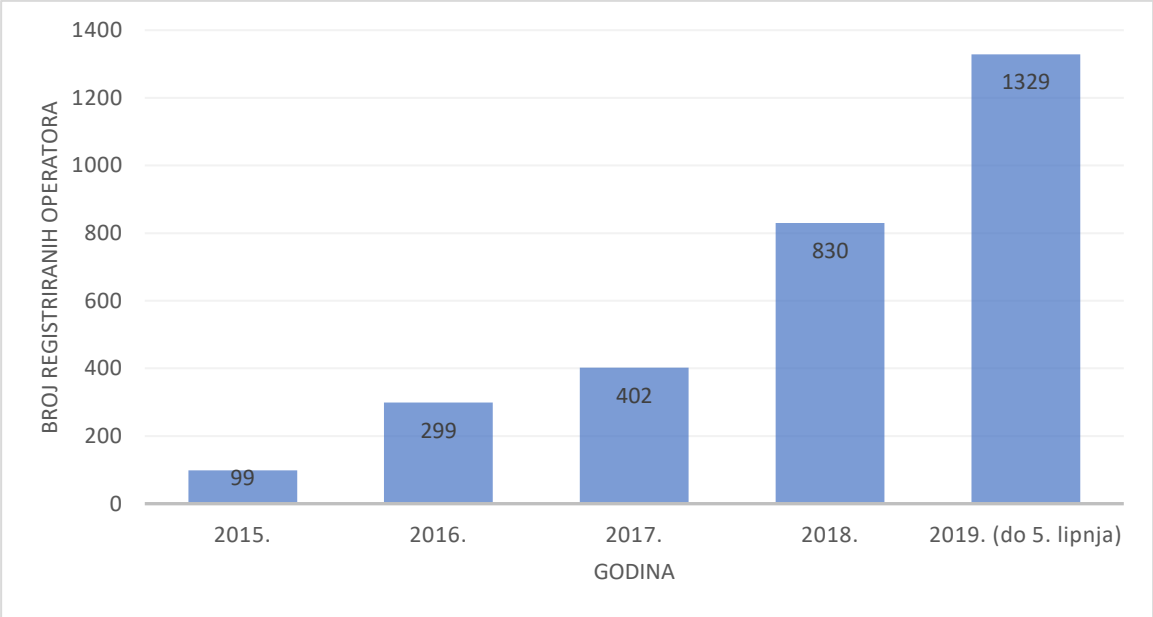
3.3. Statistički trendovi primjene bespilotnih zrakoplova u RH

Kako su bespilotni zrakoplovi sve komercijalno zastupljeniji, očekuje se njihov budući rast u svim granama privrednih i javnih djelatnosti. Neke od najčešćih grana njihove primjene su:

I. Nadzor i izviđanje
II. Hitna medicinska služba
III. Potraga i spašavanje
IV. Protupožarna zaštita
V. Agronomija (agrikultura)
VI. Dostava i transport roba
VII. Novinarstvo
VIII. Detekcija minsko-eksplozivnih sredstava

U Republici Hrvatskoj 2015. i 2016. godine započelo je bilježenje i registracija civilnih operatora koji su u vlasništvu bespilotnih zrakoplova unutar kategorija koje je potrebno registrirati. U grafikonu 1, prikazan je porast registracija aktivnih operatora bespilotnih zrakoplova u zadnjih nekoliko godina u kojem je vidljiv eksponencijalan porast operatora.

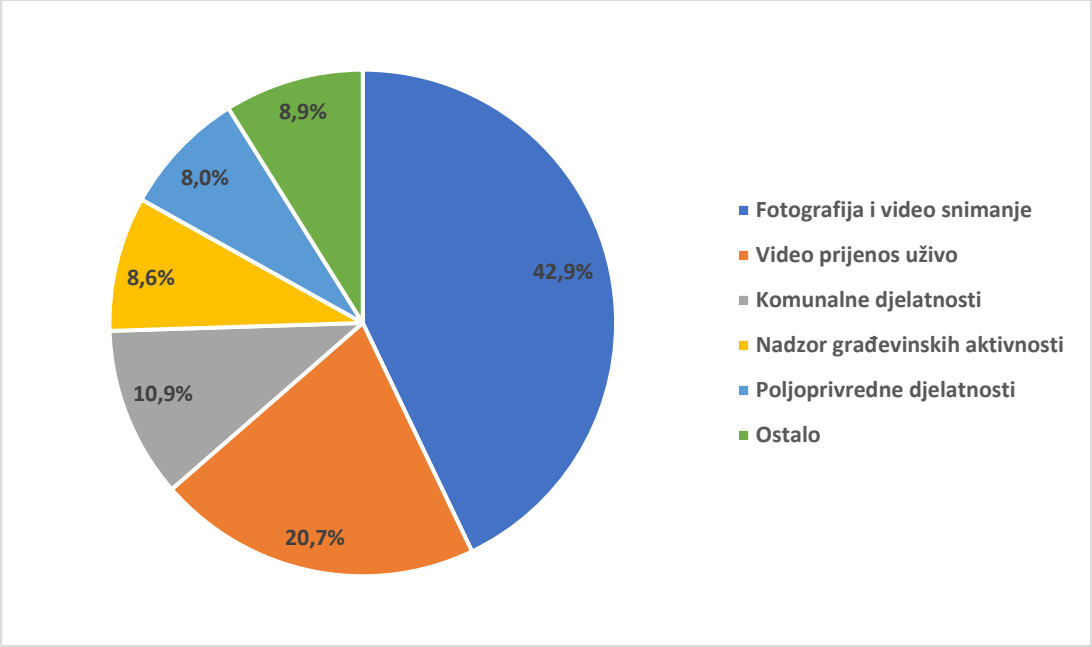
Problem u evidenciji je što ne postoji adekvatan mehanizam za bilježenje broja aktivnih letjelica te što neki letovi nisu prijavljeni te se izvode ilegalno. Dodatno, u evidenciju ne ulazi broj bespilotnih zrakoplova koji su ispod 900 grama te čak i 250 grama čiju aktivnost i postojanje po zakonu nije potrebno evidentirati.



Grafikon 1. Broj registriranih operatora bespilotnih zrakoplova u RH po godinama

Izvor: [30]

U nastavku, na grafikonu 2, slijedi prikaz nekih od najučestalijih djelatnosti u kojima sudjeluju bespilotni zrakoplovi kao jedan od njihovih mehanizama na svjetskoj razini za 2017. godinu.



Grafikon 2. Učestalost korištenja bespilotnih zrakoplova u svijetu za 2017. po pojedinoj djelatnosti

Izvor: [31]

Iz prethodnog grafa je vidljivo kako se najveći dio bespilotnih zrakoplova u svijetu koristi za aktivnosti koje uključuju kameru te snimanja bilo u privatne ili poslovne svrhe te idući trend po raširenosti korištenja iz sličnog spektra, prijenosa video sadržaja uživo. Ostale djelatnosti prema raširenosti korištenja zahvaćaju manji dio kolača jer potencijal za samu privredu i industriju još nije prepoznat od krajnjih korisnika što će se zasigurno promijeniti promatramo li ostale pokazatelje rasta.

Za sad rekreacije aktivnosti u civilnom korištenju bespilotnih zrakoplova prevladavaju zbog atraktivnosti zabilježenih zračnih snimki te lakoćom njihove distribucije na neki od mobilnih pametnih uređaja te na kraju i objavljivanjem na društvenim mrežama.

4. Sigurnosne protumjere letačkim aktivnostima bespilotnih zrakoplova

Bespilotni zrakoplovi, kao što je navedeno u prethodnim poglavljima, svojim malim dimenzijama, prihvatljivom cijenom te sa sve kvalitetnijom i ozbiljnijom dodatnom opremom (tzv. *payload*) postaju sve dostupniji što ih postavlja na mjesto potencijalnih sigurnosnih ugroza za ljude i okolinu. Uz malo tehničkog predznanja oni se mogu modificirati da nose ubojite terete primjerice u terorističke svrhe što je puno ozbiljniji problem od često javnog mišljenja kako bespilotni zrakoplovi nadziru iz zraka te narušavaju pravo privatnosti u svojoj zlouporabi.

Bez obzira na tip njihove ilegalne i zlonamjerne uporabe, potrebno je poznavati mehanizme i alate koji pomažu kod odvraćanja, sprječavanja letačkih aktivnosti i zaplijene bespilotnog zrakoplova u slučaju takvih sigurnosnih incidenata. S druge strane i gledajući problematiku iz pozitivnog kuta, bespilotni zrakoplovi su vrlo korisni kod traganja, spašavanja, nadzora, dostave dobara te u suprotnosti s nekim tradicionalnim sustavima poput npr. helikoptera, imaju prednost u početnoj cijeni te cijeni eksploatacije.

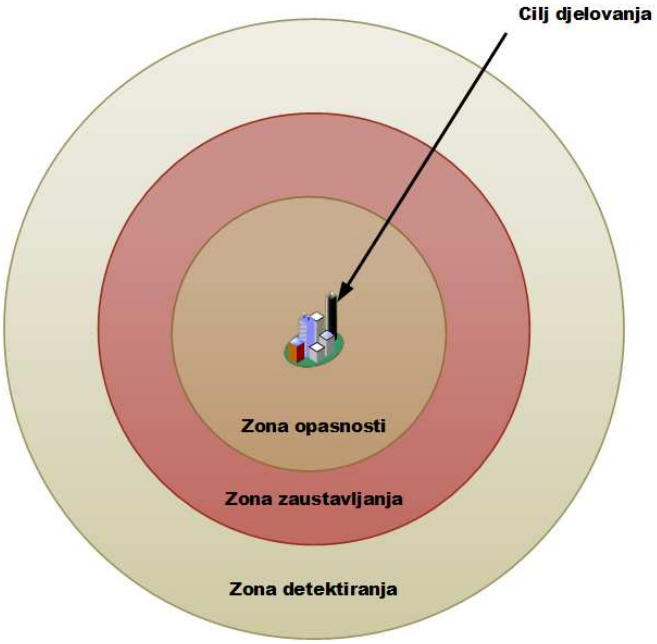
Tu postoji potencijal za zlonamjerno ometanje ili čak obaranje bespilotnih zrakoplova kod takvih zadaća. Iz tog razloga je važno poznavati obje strane spektra djelovanja, kako zaštititi ljude i okolinu od negativnog utjecaja korištenja bespilotnih zrakoplova te kako zaštititi bespilotni zrakoplov i njegove slabosti od vanjskih zlonamjernih prijetnji.

Prema nacionalnoj strategiji Velike Britanije o protumjerama uporabe bespilotnih zrakoplova, [32], u nastavku slijede primjeri prijetnji i rizika koje letačke aktivnosti bespilotnih zrakoplova predstavljaju za ljude i okolinu:

- Narušavanje zabranjenih zona letenja i kritične nacionalne infrastrukture (aktivnosti iznad područja zračnih luka, vojnih objekata, zatvora i sl.)
- Uporaba bespilotnih zrakoplova u svrhu organiziranog kriminala (dostava narkotika, oružja, komunikacija i priprema kriminalnih djela i sl.)
- Uporaba bespilotnih zrakoplova u svrhu terorističkih aktivnosti (modifikacija bespilotnih letjelica u smislu dodavanja oružja za vojno-napadačke aktivnosti, špijunažu i nadzor iz zraka, snimanje iz zraka u svrhu ilegalnih promidžbenih aktivnosti terorističkih skupina i sl.)

Iz perspektive sigurnosnih slabosti bespilotnih zrakoplova kao letjelica nameću se prijetnje neautoriziranim RF ili *Wi-Fi* pristupom letjelici u svrhu dohvaćanja podataka o njenoj konfiguraciji, izmjeni postavki i letačkih parametara, te ometanju ili promjeni navigacijskih sustava, [33].

Prije analize potencijalnih mogućnosti i sustava koji se koriste kao protumjere letačkim aktivnostima bespilotnih zrakoplova, važno je razumjeti pristup toj problematici. Svaki segment je lakše opisati ako se potencijalne zlonamjerne aktivnosti definiraju prema zonama u odnosu na krajnji cilj djelovanja bespilotnog zrakoplova.



Slika 5. Zone protudjelovanja bespilotnim zrakoplovima

Izvor: [34]

Mjere protudjelovanja mogu se razmatrati prema zonama prikazanim na slici 5. Jedan od termina koji opisuje sustav zaštite i prevencije određene točke je C-UAS (engl. *Counter-Unmanned Aerial System*).

Takav sustav, ne računajući ostale manje napredne tehnike, sastoji se od različitih visoko tehnoloških rješenja (radarske i senzorske tehnologije potpomognute specijaliziranim algoritmima, softverskim rješenjima) koja sinkronizirano funkcioniraju ali svako u vlastitoj zoni djelovanja te su često vojne namjene primjenjivi i u civilne svrhe.

Primjerice, u zoni detektiranja važno je prepoznati neidentificiranu i neautoriziranu bespilotnu letjelicu, njenog pilota na daljinu te pokušati utvrditi namjeru njenih letačkih aktivnosti. Neovisno o uspješnosti prethodne detekcije, ulaskom bespilotnog zrakoplova u zonu zaustavljanja, njegova aktivnost u zraku smatra se kao potencijalna ugroza sigurnosti te tada mogu nastupiti tehnike i mehanizmi sprječavanja leta te spuštanja takve letjelice. Ulaskom u zonu opasnosti, smanjuje se vjerojatnost zaštite, važno vrijeme kontra reakcije je sve manje a rizik od incidentnog događaja je izrazito velik.

Slika 6. Primjeri C-UAS sustava

Izvor: [34], [35]

Uzimajući sve navedeno u obzir, važno je preventivno reagirati, po mogućnosti što brže, uporabom sustava velikog dometa detekcije i mehanizama zaustavljanja.

4.1. Detektiranje bespilotnog zrakoplova

Osim vizualnog otkrivanja koje ne odaje detalje o bespilotnom zrakoplovu u blizini, za detekciju se koriste već spomenuti C-UAS sustavi. Oni se sastoje od specijaliziranih elektro-optičkih senzora za manji domet ili pak od kompleksnih radarskih (engl. *Radio Detection and Ranging*) sustava za veći domet.

Radarski sustavi imaju veliku prednost u dometu jer na njih ne utječu negativno vremenske nepogode ali zato ih odlikuje ekstremno visoka cijena. Uzimajući sve u obzir najefikasniji C-UAS sustavi su oni koji kombiniraju karakteristike jednih i drugih, [34].

<u>Radari</u>

Opće je poznata upotreba radara kod nadzora zraka, tla, i mora što u vojne što u civilne svrhe. Radari za detekciju bespilotnih zrakoplova obično su kompleksniji iz razloga što se od njih zahtjeva otkrivanje vrlo malih meta tj. obrisa koje pružaju relativno male dimenzije komercijalnih bespilotnih zrakoplova u suprotnosti s ostalim letjelicama. Kao primjer, jedan od radara koji se koristi je monostatički pulsni radar. On radi na principu korištenja jedne antene za odašiljanje i primanje jakog pulsnog signala u okolini i iz nje.

Na taj način prijem ne utječe na odašiljanje i isto se odvija bez interferencije ali njegova mana je što se prilikom izmjene načina rada (prijelaz jednog stanja u drugo) javlja tzv. praznina, sustav ne odašilje niti prima *echo* iz okoline. 1 mikro sekunda trajanja pulsa rasprostire se na 300 metara što može biti problematično ako je bespilotni zrakoplov na udaljenosti od npr. 140 metara (ukupan put signala je 280 metara) isti neće biti uočen.

Također ako je pak trajanje pulsa smanji na npr. 1 milisekundu uz iste udaljenosti, radar se neće prebaciti u stanje prijema tj. slušanja i bespilotni zrakoplov neće biti otkriven. Ovakav tip radara ograničen je zbog svoje slijepe točke, praznine. Frekvencijsko modulirani valno kontinuirani radar istovremeno odašilje i prima *echo* signal te na taj način izbjegava slijepe točke u odnosnu na pulsni radar. Ima mogućnost promjene frekvencije

na kojoj odašilje *echo* pa stoga povratni signal može biti raznolik, može vratiti različite obrise objekata iz okoline.

Mana mu je određena doza interferencije zbog istovremenog odašiljanja i prijema. Visoko frekvencijski radar ovog tipa – LIDAR (engl. *Light Detection and Ranging*) pruža visoku detaljnu sliku *echo* signala ali s obzirom na to kako je on svjetlosnog oblika, vrlo je podložan vremenskim utjecajima a ujedno i vrlo skup.

Mikro-*doppler* C-UAS radar služi za detekciju manjih objekata ali s obzirom na to kako je riječ o radaru koji radi na *doppler* principu i vraća *echo* brzih objekata, problem mu mogu predstavljati bespilotni zrakoplovi koji lebde u zraku (ili se kreću jako sporo) te isti neće biti detektirani, bit će u slijepoj točki. Također, potrebna je logika kojom se obrađuje velika količina prispjelih, očitanih *echo* podataka (vremensko ograničenje).

RF i WLAN detekcija

Ista se bazira na prijemu signala frekvencija 2,4 i 5 GHz na kojima najčešće funkcionira konekcija između daljinskog upravljača i same bespilotne letjelice. C-UAS sustavi detektiraju RF i WLAN signal koji se odašilje na određenom prostoru.

U slučaju letnih operacija bespilotnog zrakoplova na frekvencijski zagušenom području (gradsko okruženje), UAS sustavi će vrlo teško detektirati iste uz veliku ovisnost o smjeru prijema detektiranog RF i WLAN signala.

Audio senzori

S obzirom na specifičan zvuk propelera, rotora i motora kod bespilotnih letjelica u multikopter izvedbi, koji može podsjetiti na zvuk roja pčela, za detekciju se također koriste specijalizirani audio senzori, odnosno mikrofoni visoke osjetljivosti.

Njihov domet ovisi o izvedbi, a može biti od 50-tak do nekoliko stotina metara. Vrlo gusto raspoređeni mikrofoni rade na principu istovremenog prijema perioda zvučnog sinusoidnog vala na svakome od njih nakon čega se vrijeme prijema tog vala koristi kod izračuna udaljenosti bespilotnog zrakoplova.

Ovakvi senzori imaju manu u obliku fizičkog ograničenja brzine zvuka. Kao što je navedeno u izvoru [34], pri udaljenosti od 500 metara, kašnjenje zvuka iznosi 1,5 sekundu što može značiti da ako bespilotni zrakoplov leti brzinom 20 m/s, on će u tih 1,5 sekundi preletjeti 30 metara bez da je detektiran. Audio senzori iznimno su skupi te osjetljivi na vremenske nepogode posebice na vjetar.

Senzori u obliku kamera

Kamere visoke rezolucije, s optičkom stabilizacijom, auto fokusom, lećama za optičko povećanje dodatno potpomognute sustavima naprednih algoritama za prepoznavanje objekata, lica i umjetnom inteligencijom već se koriste u gradovima svijeta s velikom brojem stanovnika.

Takve kamere uz male softverske preinake u C-UAS sustavima služe da detektiranje bespilotnih zrakoplova. Mane su im rad u lošim svjetlosnim i vremenskim uvjetima (magla) uz neprecizno određivanje brzine objekta u zraku. Također ne pružaju podršku za veće domete (ograničene dostupnim optičkim povećanjem kamere).Cilj je objediniti sve potrebne senzore, radare i ostale sustave za pokrivanje što većeg područja unutar kojeg je moguće detektirati bespilotni zrakoplov. Njihovom kombinacijom eliminiraju se slabosti pojedinog elementa ali raste kompleksnost i cijena.

Također posebni algoritmi prepoznavanje objekata mogu dosta doprinijeti izradi detaljnije slike objekta, npr. točnija razlika između bespilotnog zrakoplova većih ili manjih dimenzija te ptice a dodatan problem je njihovo prepoznavanje prema načinu i brzini kretanja koje nije determinističke prirode, [34].

4.2. Mehanizmi zaustavljanja bespilotnog zrakoplova

Nakon neautoriziranog i neautenticiranog ulaska bespilotnog zrakoplova u zonu zaustavljanja, odgovarajuće stručne službe u slučaju procjene potencijalne opasnosti mogu pristupiti zaustavljanju i sprječavanju njegovih letnih aktivnosti.

U te svrhe mogu se koristiti tehnološki napredniji C-UAS sustavi za ometanje signala s mogućnošću rušenja ili različiti tipovi oružja koji mogu biti jako invazivni tj. mogu prouzročiti fizička oštećenja bespilotnog zrakoplova.

Također, vrlo je teško koristiti takva oružja kod bespilotnih zrakoplova malih dimenzija što zbog njihove česte udaljenosti a što zbog preciznosti pogotka.

Prema izvoru [34], podjela mehanizama zaustavljanja preuzeta iz američke vojske je sljedeća:

I. Informiranje
II. Ometanje
III. Hvatanje i zapljena
IV. Uništenje

<u>Informiranje</u>

Mjera informiranja pilota na daljinu da prestane s letačkim aktivnostima. Upozorenje operatoru kako je prekršio određene pravilnike letenja ili je ušao bespravno ušao u određenu zonu. Cilj je a siguran način navesti operatora da prestane s neadekvatnim letačkim aktivnostima kako se ne bi primijenile idući agresivniji mehanizmi zaustavljanja.

Problem predstavlja na koji način, kojom tehnikom i tehnologijom, pravovremeno i adekvatno obavijestiti operatora. Navedeno se uspješno provodi samo ako je operator dobronamjeran i svjestan svoje pogreške. Primjer kvalitetnog rješenja koje daje pravovremene rezultate je korištenje transpondera. Isti bi trebali biti tvornički ugrađeni u bespilotne zrakoplove te bi proizvođač morao imati ugovor s određenom organizacijom ili

institucijom kako bi one mogle ručno ili automatizirano poslati signal prema bespilotnom zrakoplovu. Isti bi zatim obradio takav signal i na daljinskom upravljaču obavijestio pilota na daljinu da prestane s određenim radnjama.

Također prilikom detekcije bespilotnog zrakoplova, transponder bi nadzornoj strani omogući dohvat identifikacijskih podataka o pilotu na daljinu Ovakav način komunikacije još nije u potpunoj implementaciji kod komercijalnih bespilotnih zrakoplova već se testno koristi kod većih letjelica specijaliziranih za određena područja rada (optimizacija, sigurnost zračnog prometa).

Ometanje

Mjera ometanja komunikacije između pilota na daljinu i bespilotnog zrakoplova. Cilj je prekinuti ili dovoljno dugo ometati komunikacijski kanal, kako bi se pilot na daljinu izgubio upravljačku kontrolu. Komercijalni bespilotni zrakoplovi često imaju sigurnosni mehanizam povratka na početno uzletno mjesto (engl. *Return to home - RTH*) ukoliko dođe do prekida komunikacije, ili pak autonomno slijeću na trenutno pogodnu poziciju (ovisno o senzorski dobivenim podacima iz okoline).

Upravo uzmicanje i udaljavanje bespilotnog zrakoplova ovim načinom iz zone zaustavljanja rezultat je ometanja ili prekida komunikacije s operaterom. Često je moguće sačuvati bespilotni zrakoplov od oštećenja ovim načinom ali ponekad prekid komunikacije i signala može dovesti do neželjenog pada i njegovog oštećenja te uništenja. Problem se javlja ukoliko je letjelica ručno izrađena te ne koristi standardizirane komunikacijske tehnologije pa sukladno tome pada vjerojatnost uspješnog ometanja signala, [33], [35].

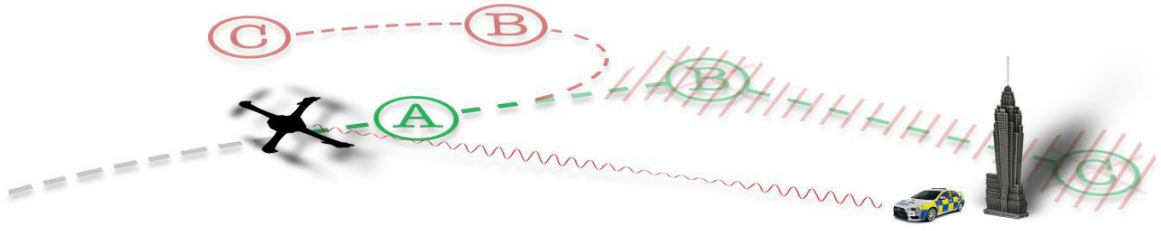
Sama tehnika ometanja temelji se na fizikalnom principu odašiljanja signala iste frekvencije ali znatno veće snage. Važno je napomenuti kako je u nekim slučajevima ilegalno RF ometanje, ovisno o korištenoj frekvenciji i snazi odašiljanja. Jednostavniji RF uređaji za ometanje su vrlo jeftini i široko dostupni te kod njih postoji problem što se ometajući signal odašilje u okolinu i ne može se njime precizno ciljati točno određeni bespilotni zrakoplov bez toga da i ostali RF uređaji iz okoline budu pogođeni tom tehnikom.

Primjer takvog napada je iskorištavanje tzv. *Backdoor* tvorničkih sigurnosnih slabosti kod komercijalnih bespilotnih zrakoplova s mogućnošću autopilot opcije. Nakon što letjelica uđe u autopilot način rada, napadač može ometati i računalom ubaciti *Maldrone* zlonamjerni softver. On zatim presreće upravljačke naredbe s daljinskog upravljača i prosljeđuje ih na lažne portove, sučelja (na transportnom mrežnom sloju). Istovremeno napadač kontrolu preuzima šaljući svoje naredbe prema bespilotnoj letjelici.

Također tehnika ometanja i preuzimanja kontrole *SkyJack* funkcionira na način da daljinski upravljač deautenticira s Wi-Fi mreže promjenom SSID-a Wi-Fi mreže te zatim na njega poveže svoje upravlja ili računalo kao zemaljsku stanicu. Za ovakav napad je potrebno uzletjeti s drugim bespilotnim zrakoplovom opremljenim Rasberry Pi računalom

te kroz linux alat *aircrack-ng* izvršiti preuzimanje. Ovako preuzet bespilotni zrakoplov naziva se kolokvijalno *zombie drone*, [33].

Druga mjera ometanja odnosi se na lažiranje koordinata s GNSS senzora za navigaciju (tzv. *spoofing*). Komunikacija se presreće odašiljanjem snažnijeg signala s drugim, lažnim lokacijskim koordinatama za različite sustave poput npr. GPS, GLONASS i sl. kako bi se postigla veća redundancija. Činjenica kako civilna GPS komunikacija nije kriptirana znatno utječe na uspješnost ovog mehanizma. Nakon toga GNSS prijemnik letjelice sinkronizira se s napadačevim GNSS odašiljačem. Rezultat je da bespilotni zrakoplov ne drži točan pravac već se kreće po novim zadanim koordinatama. Problem kod ovog načina ometanja je što ga je moguće izvesti isključivo kada se letjelica nalazi u autopilot načinu rada.



Slika 7. Princip ometanja lažiranjem GNSS koordinata, [35]

<u>Hvatanje i zapljena</u>

Mjera fizičkog hvatanja i oduzimanja bespilotnog zrakoplova na način da se isti fizički sačuva. Glavna mana ovakvog načina protumjera su što bespilotni zrakoplov mora biti u relativnoj blizini osobe koja ga želi zaustaviti hvatanjem uz mogućnost hvatanja brzih letjelica s obzirom na to kako one komercijalnog tipa bez problema dostižu brzine od 50 km/h.

Kod hvatanja popularne su ručna oružja, puške oblika sličnog ručnom raketnom bacaču koje ispaljuju mreže često s nekim oblikom padobrana kako ne bi došlo do pada bespilotnog zrakoplova nakon hvatanja. Cilj mreže je zaustaviti pogonski sklop letjelice na način da se ista oko njega omota i spriječi rotaciju propelera ili da duža mreža ostane visjeti kako bi se mogla privući s tla.

Problem ovog pristupa hvatanju je što su takva oružja za veće letjelica izrazito kompleksna i skupa te osjetljiva na vremenske uvjete poput temperature i vjetra. Drugi oblik pušaka je klasična sačmarica ali s plastičnim punjenjem patrona. Potencijalno može oštetiti bespilotni zrakoplov kao ljude i životinje u njegovoj okolini, stoga nije pogodna za gradske uvjete. Postoji primjer različitih policija i vojski koje su odabrale drugačiji pristup, hvatanje te ponekad rušenje bespilotnih zrakoplova uz pomoć treniranih orlova. Ti timovi uzgajaju i treniraju vlastite orlove na način da im od mlade dobi daju makete u obliku bespilotnih letjelica za igru.

Uništenje

Invazivna mjera, u smanjenom obujmu mehanizma protuzračne obrane, gdje se bespilotni zrakoplov zaustavlja rušenjem te vrlo često fizičkim uništavanjem. Ovakav pristup daje odgovarajuće sigurnosne rezultate, u prihvatljivom dometu ali može biti opasan i koban za ostale sudionike iz okoline, što od samog djelovanja nekim oružjem ili pak slobodnim padom bespilotnog zrakoplova.

Oružja za rušenje se najčešće u obliku lakog vatrenog oružja poput pištolja ili pušaka te kompleksnijih oružaj poput laserskih topova. Kod tradicionalnog ručnog oružja moguće je koristiti različitu municiju od klasične, balističke u kritičnim situacijama do posebne koje se rasprskava pred metom zbog smanjenja potencijalnih oštećenja bespilotnog zrakoplova. Takva municija često je izrađena od različitih materijala. Također za veće vojne bespilotne zrakoplove nije isključena uporaba manjih projektila koristeći sustave protuzračne obrane.

Tehnološki naprednija oružja za uništavanje bespilotnih zrakoplova su laserski topovi bilo u vidu ručnog naoružanja ili pak kao mobilne stanice na vozilima. Laserski topovi koriste industrijske lasere visoke snage za koncentrirano neutraliziranje manjih letjelica među koje se mogu ubrajati i bespilotni zrakoplovi.

Laserski snop dovoljno je snažan te može zapaliti kućište ili unutarnje dijelove letjelice. Odlikuje ih velik domet i preciznost bez potencijalne ugroze okoline od laserskih zraka. Problem predstavlja kompleksnost dalekosežnih sustava zbog zahtjeva velikih pogonskih sklopova koji isto omogućavaju pretvaranjem visokog napona u laser velike snage.

5. Metodologija i metode akvizicije podataka s bespilotnih zrakoplova

Pristup istraživanju tj. aktivnostima digitalne forenzike dronova vrlo je sličan digitalnoj forenzici pametnih mobilnih uređaja. Sličnost se u velikoj mjeri očituje u mogućnostima, načinima povezivanja, komunikacijskim tehnologijama, međusobnoj kompatibilnosti te na kraju i istim izvedbenim konceptima memorijske pohrane.

Kao i kod digitalne forenzike mobilnih terminalnih uređaja pristup samom procesu je vrlo bitan, gdje se nameće pitanje odabira metodologije u tom procesu. Prije njenog odabira, istražitelj se mora držati sljedećih načela te poštovati tzv. *chain of custody,* odnosno osigurati forenzički validirane dohvaćene podatke:

- Dokazi trebaju biti prikupljeni legalnim putem i sredstvima
- Osoblje koje provodi forenzičke aktivnosti treba biti pravilno educirano
- Dokazi se ne smiju izmjenjivati, ako pak postoji potreba za istim onda je to zadatak za iskusnije u samom timu koji mogu opravdati svoje postupke
- Svi postupci i akcije trebaju biti dokumentirani tako da ako treća strana prema njima izvodi istraživanje krajnji rezultat mora biti identičan

Problem kod planiranja i odabira metodologije je pronaći onu koja će maksimalno dohvatiti iz dostupnih izvora i potencijalnih dokaza. Ujedno, razne forenzičke tvrtke razvijaju vlastite metodologije pa je teško pronaći odgovarajuću. Najčešće se proces svede na kombinaciji korištenja različitih metodologija, ovisno o početku, tj. ovisno s kakvim dokazima raspolažemo najprije.

<u>Prema izvoru [36], jedan metodološki proces bi se odvijao prema sljedećem:</u>

(1) Pristupanje zaplijenjenom dronu tako da se isključi sa napajanja/baterije kako bi se onemogućilo njegovo uključivanje i eventualno automatski pokrenula pozadinska razmjena podataka i komunikacija. Također u ovom koraku je važno pripaziti na fizičke otiske prethodnih korisnika i DNA (engl. *Deoxyribonucleic acid*) uzorke koji bi se trebali izuzeti prije bilo kakvog postupka digitalne forenzike.

(2) Identifikacija i dokumentiranje fizičkih obilježja te nosećih komponenti drona poput serijskog broja i modela drona, MAC adrese, otisnutih QR (engl. *Quick Response code*) ili BAR kodova, ugrađenih komponenti poput izmjenjive kamere, *gimbal* stabilizatora te na kraju utvrđivanje i ekstrakcija podataka s unutarnje ili vanjske memorijske pohrane. Ona može sadržavati metapodatke, multimedijske datoteke, *log* zapise letova, GPS koordinate leta i uzletno-sletnih točaka, datotečni sustav, podatke s mobilne aplikacije i ostalo.

(3) Analizirati dohvaćene digitalne dokaze i artefakte kao što su *firmware*, *thumbnail* naslovne sličice, EXIF (engl. *Exchangeable Image File Format*) metapodatke, Linux datotečni sustav, aktivne te sakrivene datoteke, postavke registara te datoteke koje su povezane, tzv. *mount*-ane na datotečni sustav. Time se može doći do određenih zaključaka o slučaju uz njihovu prezentaciju trećim tijelima i organima uključenim u istragu. Prilikom prezentacije dokaza potrebno je priložiti svu dokumentaciju skupljanu tijekom procesa kako bi se u svakom trenutku moglo dokazati da niti jedan segment metodologije nije nelegalan te da su podaci dobiveni njime nepromijenjeni i u izvornom obliku.

Gledajući svaki element izvora zasebno, može se reći da određena grana forenzike služi za njegovo ispitivanje i analizu. Pritom se mogu povući sljedeće paralele, [37]:

- *Dron* / bespilotna letjelica = Forenzika Linux OS-a
- Kontroler / upravljač = Mrežna forenzika
- Memorijska pohrana = Standardne procedure digitalne forenzike
- Letačka aplikacija = Forenzika mobilnih uređaja (Android i iOS)
- *Cloud* pohrana = *Cloud* forenzika

Jedna od obuhvatnijih referentnih metodologija digitalne forenzike Android i iOS platformi, koja uključuje pažljiv pristup uređaju, manipulaciju, analizu i prezentaciju rezultata izrađena je 2011. godine unutar SANS (engl. *Escal Institute of Advanced Technologies*) instituta čija je primarna djelatnost obuka, mentoriranje i certificiranje u području informacijske i *cyber* sigurnosti. *Developing Process for Mobile Device Forensics*, kako je ime te referentne metodologije sastoji se od 9 koraka/faza.

5.1. Referentna metodologija mobilne digitalne forenzike

Ova metodologija I pristup forenzičkoj analizi pametnih mobilnih terminalnih uređaja, a tako i bespilotnih komercijalnih letjelica sastoji se od sljedećih faza, [38], [39]:

1. Uvođenje
2. Identifikacija
3. Priprema
4. Izolacija
5. Procesiranje
6. Verifikacija
7. Dokumentiranje
8. Prezentacija
9. Arhiviranje

1. Uvođenje

Na ovoj razini procedura obuhvaća predaju uređaja na laboratorijsko ispitivanje te njemu pripadajuću dokumentaciju vezanu uz vlasništvo uređaja, tipu i vrsti incidenta u koji je isti uključen te na temelju tog incidenta vezanu dokumentaciju uz specifične vrste podataka koje je potrebno dohvatiti iz tog uređaja. U ovoj fazi određuju se zahtjevi i ciljevi laboratorijskog ispitivanja uz maksimalnu privrženost prikupljanja i dokumentiranja svih kritičnih radnji u svrhu očuvanja lanca posjeda dokaza i njegove neporecivosti.

2. Identifikacija

Kod faze identifikacije, digitalni forenzičar mora jasno i koncizno razumjeti pravno-zakonsku regulativu područja u kojem radi te razumjeti što se od njega traži u dobivenom sudskom nalogu te koje su njegove ovlasti. Nadalje, vrlo bitno je odrediti ciljeve cijele istrage prema mogućnostima laboratorija, korištenih alata i znanja pojedinca ili tima istražitelja. Ti realni ciljevi jasno će prikazati što je moguće dohvatiti a što ne prema tehničkim karakteristikama korištene opreme ali i ispitivanog uređaja.

Također iz tog razloga nužno je identificirati ispitivani uređaj prema modelu, standardiziranim identifikatorima (ESN – engl. *Electronic Serial Number*, MEID – engl. *Mobile Equipment Identifier*, IMEI, ICCID – engl. *Integrated Circuit Card Identifier*, MSISDN - engl. *Mobile Station International Subscriber Directory Number* i sl.) i karakteristikama zbog odabira odgovarajućih forenzičkih alata.

3. Priprema

Nakon identifikacije potrebno je odrediti koji forenzički alati će se koristiti, u kojem obujmu te na koji način s obzirom na prethodno utvrđene karakteristike analiziranog uređaja. Uz odabir forenzičkih alata, u ovom koraku nužno je pribaviti i osigurati svu opremu poput softvera, hardvera, kablova bez kojih prijenos ekstrahiranih podataka te povezivanje na uređaj nije moguć. Uz sve navedeno, prilikom pripreme odabire se najpogodnija metodologija ekstrakcije koja će biti kasnije korištena.

4. Izolacija

Izolacija u ovom koraku podrazumijeva onemogućavanje komunikacije između ispitivanog uređaja i informacijsko-komunikacijske mreže ili onemogućavanje povezivanja s drugom uređajima iz okoline. Neke od komunikacijskih tehnologija mogu omogućiti udaljen pristup ispitivanom uređaju te u konačnici izmjenu ili uklanjanje podataka s njega što može dovesti do kompromitacije krajnjih rezultata forenzičke istrage.

Također kako bi se spriječile nenamjerne pogreške brisanja, kopiranja ili premještanja podataka od strane ispitivača, važno je uređaj izolirati i onemogućiti takav način njegove komunikacije. U tu svrhu koriste se folije, vreće, kavezi, torbe pa čak i sobe temeljene na principu Faradayevog kaveza ili uređaji za ometanje radio signala koji blokiraju elektromagnetske valove.

Problem kod izolacije je povećana potrošnja električne energije iz baterije uređaja koji se samostalno pokušava priključiti na neku mrežu, stoga je nužno osigurati konstantno i odgovarajuće napajanje kako bi se izbjeglo gašenje uređaja i potencijalan gubitak podataka iz stalne ili privremene memorije.

5. Procesiranje

U ovoj fazi započinje se postupak ekstrakcije podataka iz uređaja. Prvo je potrebno ukloniti svu vanjsku pohranu te mrežnu karticu ukoliko postoje, te podatke s njih dohvatiti zasebno. Ako nije moguće odvojiti vanjsku pohranu i mrežnu karticu te ih posebno analizirati iz bilo kojeg razloga, tu činjenicu potrebno je naglasiti u formularima i dokumentaciji. Preporučljivo je provesti što je više moguće ekstrakcijskih metoda kako bi se prilikom analize mogla stvoriti šira slika dokaza te povećala vjerojatnost pronalaska istih.

6. Verifikacija

Prilikom izvođenja forenzičke analize važno je osigurati tzv. lanac očuvanja prikupljenih dokaza (engl. *chain of custody*), odnosno izvršiti analizu bez izmjene podataka na uređaju. Očuvanje izvornog oblika digitalnih dokaza postiže se njihovom verifikacijom.

Prvi način verifikacije odnosi se na usporedbu podataka izvornih s uređaja te podataka koji su s istog dohvaćeni. Drugi način se provodi koristeći višestruke ekstrakcije putem različitih forenzičkih alata te u konačnici usporedbom njihovih rezultata. Treći i posljednji način verifikacije provodi se tzv. *hash* funkcijom koju većina današnjih alata provede nad podacima te oni budu jedinstveno opisani i identificirani. Usporedbom i utvrđivanjem identične *hash* vrijednosti kod ekstrahiranih i izvornih podataka, može se utvrditi kako oni nisu mijenjani i kako su neporecivi.

7. Dokumentiranje

Za vrijeme trajanja cijelog postupa forenzičke istrage, svaki korak treba biti valjano dokumentiran. Dokumentacija se obavlja prikupljanjem bilješki, često kroz razne formulare i predloške koji imaju za cilj jasno pružiti informaciju o tome tko je sudjelovao u istrazi, koji alati su korišteni, koji podaci su dohvaćeni, koji ciljevi su uspješno postignuti i sl. Neki od podataka koje je bitno evidentirati su: datum i vrijeme početka te kraja istrage (važno je ispravno uskladiti vremensku zonu i standarde između uređaja i alata s obzirom na to kako uređaj može imati svoje lokalno podešeno vrijeme i datum), zaprimljeno stanje uređaja te opreme uz opis i slike, fotografije identifikatora uređaja, informacije o korištenom forenzičkom alatu te dohvaćenim podacima.

8. Prezentacija

Svi dohvaćeni podaci nakon pravilnog dokumentiranja moraju biti složeni i prebačeni u oblik koji je jasan i razumljiv ne samo ostalim forenzičarima već i ostalim sudionicima koju su uključeni u istragu poput sudaca, vještaka tj. sudionika koji nemaju toliku razinu tehničkog znanja. Takva prilagođena dokumentacija obično se predaje u digitalnom obliku ili pak elaboratu koji kasnije mogu biti dodatno analizirani bilo ručno ili softverski. Dokazi poput SMS poruka, fotografija i sl. vizualno moraju biti jednostavni i intuitivni za pregled ostalim ne stručnim sudionicima.

9. Arhiviranje

Bilo da je slučaj zaključen ili da je još u postupku, svu prikupljenu dokumentaciju važno je arhivirati. Ponekad će postojati potreba ponovo ustupiti dokaznu dokumentaciju u svrhu žalbi ili novih, dodatnih sudskih postupaka. Također u slučaju budućih sličnih postupaka, prijašnja dokumentacija može poslužiti i pomoći kao referentni model (sa standardiziranim formatom podataka), [38], [39].

5.2. Metode ekstrakcije digitalnih dokaza

Sama ekstrakcija podataka spadala bi prema redoslijedu u 5. fazu referentne metodologije, u fazu procesiranja. Kada se govori o ekstrakciji ili akviziciji podataka, tad se pod time misli na analiziranje određenih, dostupnih tipova memorijske pohrane pomoću forenzičkog alata te na prikupljanje podataka pronađenih na toj memoriji.

Podaci se ne uklanjanju s memorije već ih se kopira na siguran forenzički način te pohranjuje prema najboljoj praksi na forenzički čist i nekontaminiran medij. Jednostavnije metode obično vremenski traju kraće, prikupe manji set podataka, nije ih kompleksno za izvoditi te ne zahtijevaju sofisticirane i skupe forenzičke alate. Složenije metode su kompleksnije za izvođenje, traju puno duže jer prikupe veći set podataka, zahtijevaju stručnost, znanje te skupe forenzičke alate.

Prema izvorima [38], [40], [41], metode ekstrakcije ponekad zahtijevaju otvaranje uređaja što može biti jako invazivno te u konačnici rezultirati prestankom njegova rada. Takve metode su zadnja opcija ukoliko istražitelj manje invazivnim metodama dohvati ciljanu skupinu podataka.

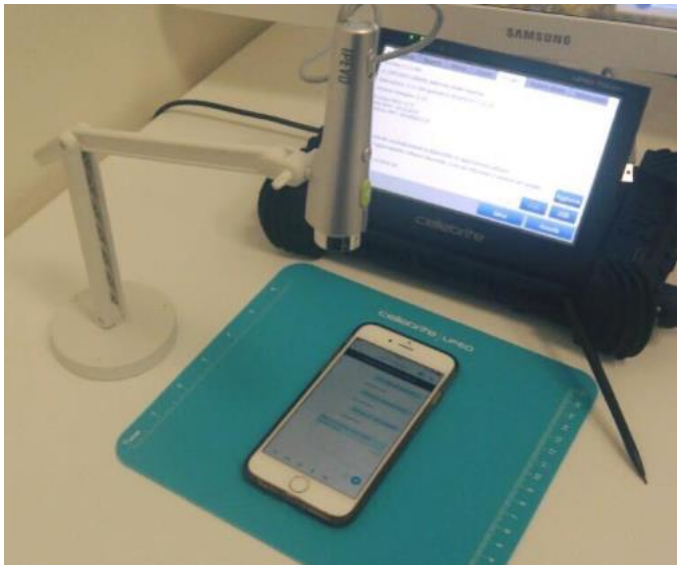
Metode ekstrakcije, od manje invazivnim prema invazivnijim, dijele se na:

a. Ručna ekstrakcija
b. Logična ekstrakcija
c. Datotečna ekstrakcija
d. Fizička ekstrakcija (*Hex Dump* / JTAG, Chip-off, Micro Read)

Ručna ekstrakcija

Ova metoda se zasniva na klasičnom korištenju uređaja, tj. korištenju njegovih ulaznih komponenti za otvaranje, kretanje i izvođenje radnji kopiranja kako bi se dohvatili digitalni dokazi. Preko tipkovnice, zaslona ili nekog drugog oblika hardvera pregledom sadržaja uređaja može se jednostavno doći do dokaznog materijala uz vrlo čest uvjet, da sam uređaj bude otključan. Prikupljen sadržaj pohranjuje se na vanjski medij ili se zaslon snima posebnim forenzičkim kamerama odnosno skenira u radu.

Neke od prednosti ove metode su jednostavnost, često podržana od većine uređaja, gdje nisu potrebni specijalizirani kablovi i oprema. Nedostatci se očituju u dugotrajnosti cijelog postupka, moguće je promijeniti izvorne podatke, dohvaćanje ograničenog seta podataka, poteškoće u izvođenju (postavke uređaja, jezik, zaključan pristup), [38], [40], [41].



Slika 8. Primjer izvođenja i snimanja ručne ekstrakcije, [40]

Logička ekstrakcija

Logička ekstrakcija provodi se povezivanjem ispitivanog uređaja te radne stanice. Povezivanje je najčešće putem pripadajućeg kabela. Radnu stanicu predstavlja računalo ili drugi hardverski forenzički alat koji u sebi mogu ili ne moraju imati instaliran specijaliziran forenzički alat u obliku softverskog rješenja. Forenzički alat distribuira naredbe koje uređaj procesira i na radnu stanicu vrati sadržaj svoje pohrane. U te podatke ulaze vidljiv sadržaj koji je alociran na memoriji, često neobrisan, te stvara forenzički sliku datotečnog sustava uređaja. Dubina prodiranja u datotečni sustav ovisi o tome postoji li na uređaju omogućen korijenski, *root* pristup ili ne. Uz datotečni sustav logička ekstrakcija može prikupiti i kreirane sigurnosne kopije podataka i postavki uređaja (neki alati prvotno kreiraju sigurnosnu kopiju pa ju zatim dohvaćaju).

Prednosti ovog pristupa su moguća ponavljanja, jednostavnost izvođenja, brzina i veći set podataka od ručne ekstrakcije, dok su mane potreba posebnih i specijaliziranih kablova za određene uređaje, potencijalne izmjene nekih datoteka (SMS – engl. *Short Message Service*), ne dohvaćanje ne alociranog memorijskog prostora te nemogućnost izvođenja na zaključanim uređajima.

Postoje dva načina izvođenja logičke ekstrakcije:

I. Agentska logička ekstrakcija

Na uređaj se preuzme ili putem radne stanice distribuira forenzički alat u obliku aplikacije/softvera koji nakon pokretanja prikupi prethodno opisane podatke, pošalje ih na vanjsku pohranu ili radnu stanicu, zatvori i kod završavanja deinstalira s uređaja

II. Ekstrakcija putem *Android Debug Bridge (ADB)* naredbi

Na uređaju kroz postavke prethodno mora biti omogućena opcija *USB debugging* te zaslon mora biti otključan (onemogućeno zaključavanje uređaja). Nakon kreiranja tzv. „mosta“, forenzički alat prikuplja prethodno pisane podatke na vanjsku pohrani ili radnu stanicu.

Datotečna ekstrakcija

Datotečna ekstrakcija je zapravo dio logičke akvizicije s većim setom prikupljenih podataka. Glavna razlika u odnosu na logičku ekstrakciju je da prilikom dohvata datotečnog sustava sam pristup podacima se odvija izravno, a ne putem protokola vezanih uz operativni sustav, aplikacijskim sučeljima (API - engl. *Application Programming Interface*).

Digitalni dokazi dohvaćeni su u obliku sistemskih datoteka, *log* zapisa te baza podataka. Ti podaci često imaju svoje metapodatke te ako istražitelj izvodi ručno dohvaćanje putem SQL (engl. *Structured Query Language*) naredbi kroz bazu podataka, moguće ih je otkriti kao izbrisane, sakrivene ili privremene. Za takav ručni pristup potreban je veći dijapazon znanja kod istražitelja, [42], [43].

Fizička ekstrakcija

Fizička ekstrakcija spada u najsloženiju metodu za koju su obično potrebni napredniji i skuplji forenzički alati. Ona omogućuje potpuni pristup i alociranoj i ne alociranoj memorijskoj pohrani te je u mogućnosti dohvatiti posebno željene korisnički obrisane datoteke i podatke.

Forenzičkim alatom ostvaruje se potpun pristup uređaju otključavajući dio operativnog sustava zaduženog za njegovo pokretanje tzv. *bootloader*. Nakon toga forenzički alat putem svojih *proprietary* mehanizama ili *backdoor* metoda dolazi do pristupa memorijskom čipu iz kojeg se zatim dohvaćaju podaci.

Na vanjski medij ili radnu stanicu set podataka s memorije se pohrani u jednu datoteku .img ekstenzije koja se zatim ponovo može analizirati i dekodirati istim ili drugim forenzičkim alatima. Samo dohvaćanje podataka s memorije odvija se po njenim sektorima i to tzv. bit po bit gdje se dohvaća izvorna vrijednost podataka u obliku binarnog zapisa 0 i 1. Ova metoda je vrlo složena jer forenzički alat mora imati mehanizme zaobići sigurnosne značajke operativnog sustava te hardvera te zbog *bit-by-bit* principa vrlo dugotrajna.

Također vrijeme izvođenja ovisi i o hardverskim karakteristikama radne stanice na kojoj se izvodi forenzički alat ali i o ukupnom kapacitetu memorijskog čipa ispitivanog uređaja. Kako se kod fizičke ekstrakcije koriste posebni protokoli, dekriptiranje, digitalni potpisi te obrnuti inženjering alati koji ju omogućuju nisu *open-source* tipa i vrlo su skupi.

Invazivni pristup uključuje pristup uređaju na razini elektroničkih komponentni i sklopova odnosno njegovo otvaranje. Nakon izvođenja takve akvizicije uređaj potencijalno može ostati neuporabljiv. Pristup matičnoj ploči uređaja zahtjeva posebne alate i vještine njihovim rukovanjem kako ne bi došlo do nenamjernog oštećivanja i uništavanja memorijskih modula.

Slika 9. Primjeri Chip-Off i JTAG tehnika

Izvor: [44], [45]

Neke od invazivnih metoda su prema izvorima [41], [46] su:

- *Hex Dump* / JTAG (engl. *Joint Test Action Group*)

  Metoda koja kabelskom vezom, određenim specijaliziranim softverom, uklanjanjem memorijskog modula sa SoC-a (engl. *System on a Chip*) ili povezivanjem na SoC specijaliziranim kablovima na točno određena konekcijska mjesta (TAP - engl. *Test Access Ports*) može dohvatiti tzv. sirove podatke koje treba interpretirati i pretvoriti u razumljiv oblik.

  Ograničenja su: potrebna posebna konverzija podataka, složenost izvođenja, posebno izrađena oprema i kablovi, hardverska ograničenja proizvođača uređaja.

- Chip-Off

  Kako i samo ime govori, ovom metodom se uklanja memorijski modul sa SoC-a te se njegov sadržaj zatim očitava putem drugog uređaja ili tzv. *EE prom* čitača. Ograničenja su vrlo slična i kod prethodno opisane metode ali ovdje dodatni problem stvara mogućnost nabave točnog čitača za određeni tip memorijskog modula kao i činjenica da ekstrahirani podaci nisu sortirani po redoslijedu. U toj kompleksnosti bitova teško je odrediti koji bit odgovara kojem podatku. Uz opasnost uništavanja čipa, ova metoda je vrlo skupa za izvođenje, zahtjeva posebna znanja i vještine kod interpretiranja rezultata.

- Micro Read

  Najzahtjevnija metoda koja je vremenski najdugotrajnija. Koristi se kod oštećenih memorijskih modula kako bi specijaliziranim elektroničkim mikroskopom ručno dobio pristup i uvid u njegovu strukturu. Zahtjeva vrsno poznavanje logike i principa rada memorijskih modula kako bi se rezultati zatim mogli ispravno interpretirati. Sama složenost ovog postupka navodi istražitelje da prvotno pokušaju sve prethodne metode koje su u današnje vrijeme dovoljno uznapredovale. Micro Read nije praktična metoda iako pruža najveći set podataka te je rezervirana samo za ekstremne slučajeve poput ugroza primjerice nacionalne sigurnosti.

6. Forenzička analiza bespilotnog zrakoplova DJI Mavic Air

Kao praktični dio ovog diplomskog rada u nastavku će biti prikazan proces forenzičke analize bespilotnog zrakoplova DJI Mavic Air. Cijeli postupak operativnog leta, ekstrakcije i analize podataka proveden je na području znanstveno učilišnog kampusa Borongaj te u Laboratoriju za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava.

Velik dio pripadajuće opreme te forenzičkih alata korištenih za potrebe ovog diplomskog rada dostupan je unutar spomenutog laboratorija. U nastavku slijedi tablični prikaz korištene opreme i alata:

Tablica 3. Korištena oprema prilikom provedbe forenzičke analize DJI Mavic Air-a

Oprema / alat	Opis	Namjena
DJI Mavic Air + 3 baterije	Unutarnja i vanjska pohrana	S/N: 0K1CGCERAJ2AZA
DJI daljinski upravljač	HW upravljanje	Upravljanje
Vanjski medij - HDD	1 TB	Pohrana dohvaćenih podataka
USB kabel	Tip C (*cable 170*)	Povezivanje i prijenos podataka
Sony Xperia Z1	*Root* pristup (Android 10)	Pohrana trenutnih podataka o letu i besp. zrak.
DJI GO 4 App	SW upravljanje	Prikaz trenutnih podataka o letu i besp. zrak.
Forenzička radna stanica	Windows OS	Prijenos i analiza podataka
UFED Touch 2 (UFED Physical Analyzer) V7.33.0.95	Forenzički alat	Akvizicija podataka
UFED Reader V7.33.0.30	Forenzički alat	Analiza podataka
DatCon V4.0.4	Analitički alat	Konverzija dohvaćenih podataka
CsvView V4.0.4	Analitički alat	Interpretacija dohvaćenih podataka

Kako DJI Mavic Air za upravljanje i sinkronizaciju koristi vlastitu aplikaciju DJI GO 4 App, vrlo bitna stavka kod odabira uređaja bila je podržanog istog kroz navedenu aplikaciju. S obzirom na okolnosti, od uređaja je bio dostupan Sony Xperia Z1. Prvi problem se pojavio jer je njegova verzija Android OS-a bila 5.1.1 dok je za preuzimanje i instalaciju DJI Go4 aplikacije potrebno imati uređaj s verzijom Android OS-a 6.0.

Kako bi se zaobišlo navedeno, uređaju je prvotno omogućen *root*, korijenski pristup, što je također pozitivno jer većina forenzičkih alata može dohvatiti više podataka ili pak one usko vezane uz jezgru operativnog sustava. Nakon omogućavanja *root* pristupa, na uređaju je instaliram prilagođena inačica Android-a 10, popularni LineageOS u verziji 17.1. čime je ujedno uklonjen sav sadržaj s memorijske pohrane uređaja. Podizanje sustava s 5.1.1. na 10.0 verziju, omogućilo je instalaciju i korištenje DJI GO 4 aplikacije.

Slika 10. DJI Mavic Air uz daljinski upravljač te uređaj Sony Xperia Z1

Idući korak kod planiranja simulacije letačkih aktivnosti bio je odabrati lokaciju te okvirno postaviti scenarij uz bilježenja vremena njegovih aktivnosti. Ta evidencija vremena služi kao validacija konačnog rezultata dobivenog nakon ekstrakcije i analize.

Slika 11. Prikaz okruženja prilikom izvođenja letačkih operacija

Prije samog leta nad bespilotnim zrakoplovom DJI Mavic Air provedena je procedura postavljanja na tvorničke postavke, tzv. cjelovit *factory system reset*. Zatim su formatirane unutarnja i vanjska SD pohrana na sistemski format FAT32 (engl. *File Allocation Table*) te je preko DJI GO 4 aplikacije ažuriran *firmware* bespilotne letjelice. U konačnici pripreme odrađena je jedna simulacija različitih letačkih operacija.

Scenarij letačkih operacija i operacija snimanja iz zraka odvijao se prema sljedećim točkama uz vremenske oznake:

i.	Kalibracija kompasa bespilotnog zrakoplova	14:12h
ii.	Početak leta	14:16h
iii.	Zamjena baterije	14:22h
iv.	Snimanje fotografije i video zapisa (interna i SD pohrana)	14:29h
v.	Promjena režima rada u tzv. „Sport mod“	14:30h
vi.	Brisanje video sadržaja s interne i SD pohrane	14:45h
vii.	Brisanje fotografija s interne i SD pohrane	14:46h

Kod odabira forenzičkog alata odluka je pala na Cellebrite UFED Touch 2, komercijalni hardverski alat koji se koristi u sklopu istraživanja Laboratorija za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava. Ovaj alat sastoji se od dodatnih licenciranih softverskih rješenja poput UFED Physical Analyzer, UFED Phone Detective, UFED Reader te mu je primarna namjena analiza mobilnih pametnih uređaja.

Sam UFED Touch 2 je korišten uz mentorstvo i nadzor dr.sc. Siniše Husnjaka. To je alat tvrtke Cellebrite koja je jedna od vodećih na području razvoja rješenja i alata digitalne forenzike. UFED Touch „ rješenje sastoji se od hardverske komponente, seta pripadajućih kabela te softverske komponentne u vidu slijedećih alata:

- UFED Physical Analyzer – dekodiranje, analiza i izvještaji
- UFED Phone Detective – brza detekcija mobilnog uređaja
- UFED Reader – kreiranje forme izvještaja za ostale sudionike u slučaju

UFED Physical Analyzer najvažniji je alat od navedenih, koristi se za provedbu neinvazivnih metoda ekstrakcije poput logičke, datotečne te fizičke ekstrakcije. Uz sam dohvat podataka pruža mogućnosti poput dekodiranja memorijske slike uređaja, kreiranja analitike projekta, grafički prikaz vremenske crte, izvoz podataka te kreiranje izvještaja za daljnju analizu.

Podržava velik broj proizvođača i modela pametnih mobilnih uređaja, bespilotnih zrakoplova u manjoj mjeri (DJI te Parrrot) te GPS uređaja, [47], [48]. Uz standardne *log* zapise najveća prednost je mogućnost prikaza izbrisanih podataka (ovisno o uređaju i modelu), detekcija zlonamjernog softvera, kloniranje SIM (engl. *Subscriber Identity Module*) modula i sl.

6.1. Akvizicija podataka s DJI Mavic Air

Akvizicija podataka započeta je na bespilotnom zrakoplovu DJI Mavic Air, njegovim povezivanjem s UFED Touch 2 uređajem. Za DJI Mavic Air podržane su dvije metode ekstrakcije, djelomična datotečna te fizička ekstrakcija od kojih su obje provedene. Važno je napomenuti kako za vrijeme izvođenja ekstrakcije i spremanja *image* datoteke na vanjski medij za pohranu, bespilotni zrakoplov treba biti uključen uz barem natpolovični kapacitet baterije.

Slika 12. Izvođenje ekstrakcije pomoću UFED Touch 2 alata

Nakon obje ekstrakcije, bespilotni zrakoplov dodatno je povezan na računalo te je navigacijom kroz datotečni sustav ostvaren pristup direktorijima s multimedijskim podacima na unutarnjoj i na vanjskoj SD pohrani. Ovakav klasičan *file transfer* može se promatrati kao oblik logičke ekstrakcije podataka tj. dohvata sadržaja datotečnog direktorija preko forenzičke radne stanice.

Prilikom dohvaćanja podataka uočeno je kako DJI Mavic Air na oba tipa pohrane fotografije sprema u formatu .JPG a videozapise u formatu .MP4. Putanja pohranjenih podataka je u datotečnom sustavu je /DCIM/100MEDIA gdje se uz spomenute podatke nalaze i datoteke formata .SRT koje su nusprodukt snimljenih videozapise te ih obogaćuju dodatnim metapodacima.

Također svi multimedijski podaci spremaju se pod formatom imena „DJIxxxx.format“ npr. DJI9999.MP4 ili DJI9999.JPG.

Kako je i daljinski upravljač krucijalan kod korištenja bespilotne letjelice, pretpostavka je bila da se određeni spektar digitalnih dokaza može pronaći i na njemu. Nakon višestrukih pokušaja povezivanja daljinskog upravljača na UFED Touch 2 te na radnu stanicu, niti jedan od tih uređaja nije ga uspio prepoznati. Daljnja istraživanja daljinskog upravljača nisu provođena te s njega nisu dohvaćeni podaci ni u kojem obliku.

Image Hash Details (1)

Extraction images are verified.

#	Name	Info	
1	FileDump Verified	Path	Drone_DJI - Mavic Air.zip
		Size (bytes)	62927804
		SHA256	7677BF4F7CBD679A5345506C990EA9CC87D770ACD885C72444F3AF076 02950F6

Data Files (1320)

Archives (6)

#	File Info		Additional file info		Deleted
1	MD5:	b97a6319e7036a0a9bfaddd576bddfb6	Size (bytes):	81105	
	SHA256:	1f6ca3acf59741e2b46c29a7b65da3bf 251073617212f9711ed69e8f08b5049e			
	Duplicates(1)				
	No. of files:	0			
1(1)	Name:	NOTICE.html.gz	Modified:	1/1/1970 12:00:00 AM(UTC+0)	
	Path:	Drone_DJI - Mavic Air.zip/etc/NOTICE.html.gz	Source file	Drone_DJI - Mavic Air.zip/etc/NOTICE.html.gz : 0x0 (Size: 81105 bytes)	
	No. of files:	0			
1(2)	Name:	NOTICE.html.gz	Modified:	1/1/1970 12:00:00 AM(UTC+0)	
	Path:	Drone_DJI - Mavic Air.zip/system/etc/NOTICE.html.gz	Source file	Drone_DJI - Mavic Air.zip/system/etc/NOTICE.html.gz : 0x0 (Size: 81105 bytes)	
	No. of files:	0			

Slika 13. Prikaz *hash* vrijednosti za *dump* datoteku datotečne ekstrakcije

Nakon svake izvedene ekstrakcije UFED Touch 2 dodijeli *hash* vrijednost *image* datoteci te njenim pod elementima. Za navedeno UFED Touch 2 koristi SHA-256 *hash* algoritam.

6.2. Akvizicija podataka sa Sony Xperia Z1

Uređaju je prije samog leta u fazi pripreme omogućen *root* pristup putem popularnog *root* alata Magisk. Taj alat je prema forenzičkoj zvučnosti pogodan za korištenje jer omogućuje tzv. *Systemless root*, odnosno omogućuje korijenski pristup bez direktnog modificiranja koda sistemske jezgre. Nalazi se na particiji za podizanje operativnog sustava (*boot* particija) te se s nje izvodi te ga na taj način ugrađeni sigurnosni mehanizmi Android OS-a ne mogu detektirati. Određeni drugi *root* alati izvode se na način da za potrebe ostvarivanja korijenskog pristupu izmjene sistemske datoteke, što u vidu digitalne forenzičke istrage narušava kontekst validacije i potrebit principi ne izmjenjivosti podataka, [49].

Format izvođenja ekstrakcije s pametnog mobilnog uređaja bio je istovjetan onome vezanom uz bespilotni zrakoplov. Važno je napomenuti kako je prilikom ove ekstrakcije u uređaju nije bilo vanjske SD memorije iako je ista podržana. Korišteni uređaj pronađen je od strane UFED Touch 2 uređaja, uz dodatne informacije o verziji operativnog sustava, sigurnosne zakrpe, IMEI identifikacijskog broja, tipu memorijskog modula (*chipset*) te broju instaliranih aplikacija. Vrlo bitna stavka je prikaz stanja vezanog uz korijenski pristup što je u ovom slučaju alat prepoznao.

Za ovaj mobilnih telefon podržane su: napredna logička ekstrakcija, datotečna ekstrakcija te fizička ekstrakcija. Specifične mogućnosti ima isključivo datotečna ekstrakcija koja nudi dva pristupa dohvaćanju: koristeći ADB povezivanje te kreiranje Android sigurnosne kopije koja se zatim ekstrahira.

U *log* zapisu te fizičke ekstrakcije navedeno je kako istu nije u mogućnosti provesti zato što je na uređaju verzija Androida 10, dok je prema alatu podržana samo zadnja tvornička verzija 5.1.1. Rezultat je bio dohvat podataka putem logičke i datotečne ekstrakcije. Analogno postupku bespilotnog zrakoplova, svaki set dohvaćenih podataka proveden je kroz *hash* funkciju algoritmom SHA-256.

6.3. Analiza ekstrahiranih podataka

U nastavku slijedi prikaz analize rezultata faze ekstrakcije prema ručnom pregledu podataka i pregledu kroz Cellebrite UFED alate.

6.3.1. Analiza podataka dostupnih ručnom navigacijom uređaja

Prije počinjanja analize ekstrahiranih podataka putem Cellebrite UFED uređaja, u ovom dijelu prvo će biti iznesena analiza ručno dostupnih podataka dohvaćenih kroz tzv. *file transfer* mod za bespilotni zrakoplov te za mobilni uređaj.

DJI Mavic Air

Kod bespilotnog zrakoplova pronađene su fotografije i videozapisi te već spomenute datoteke formata .SRT kojima se može pristupiti. Ove datoteke su istog imena kao i snimljeni videozapisi te prikazuju više detalja vezanih za pojedini video zapis.

Detalji tj. metapodaci podijeljeni su prema snimljenim slikama u sekundi (engl. *Frames*) a daju informacije postavkama senzora kamere (ISO, *shutter*, *color_md*), vremenu snimanja i datumu te o veličini teksta. Taj format datoteka je moguće pregledati tekstualnim uređivačima a koncept je sličan podnaslovima kod filmova.

Slika 14. Primjer prikaza .SRT datoteke u jednoj slici videozapisa

Dodatne datoteke koje je moguće ručno pronaći su datoteke formata .THM. To su zapravo fotografije, jako niske rezolucije koje se koriste kao naslovne sličice pri manipulaciji letačkom aplikacijom (engl. *thumbnail*).

Uz navedene podatke, moguće je pronaći zanimljivu datoteku formata .GIS koja aludira na podatak vezan uz geografski informacijski sustav (engl. *Geographic Information System*). Detaljnije informacije o navedenom formatu i mogućnostima interpretacije nisu pronađene.

<u>Sony Xperia Z1</u>

Prilikom ručnog pregleda uređaja uočeno je kako letačka aplikacija DJI GO 4 sve datoteke sprema u zasebnu „DJI“ mapu. Izvan toga moguće je pronaći tzv. *debug_log* zapis koji se kreira nakon povezivanja uređaja i bespilotnog zrakoplova putem daljinskog upravljača.

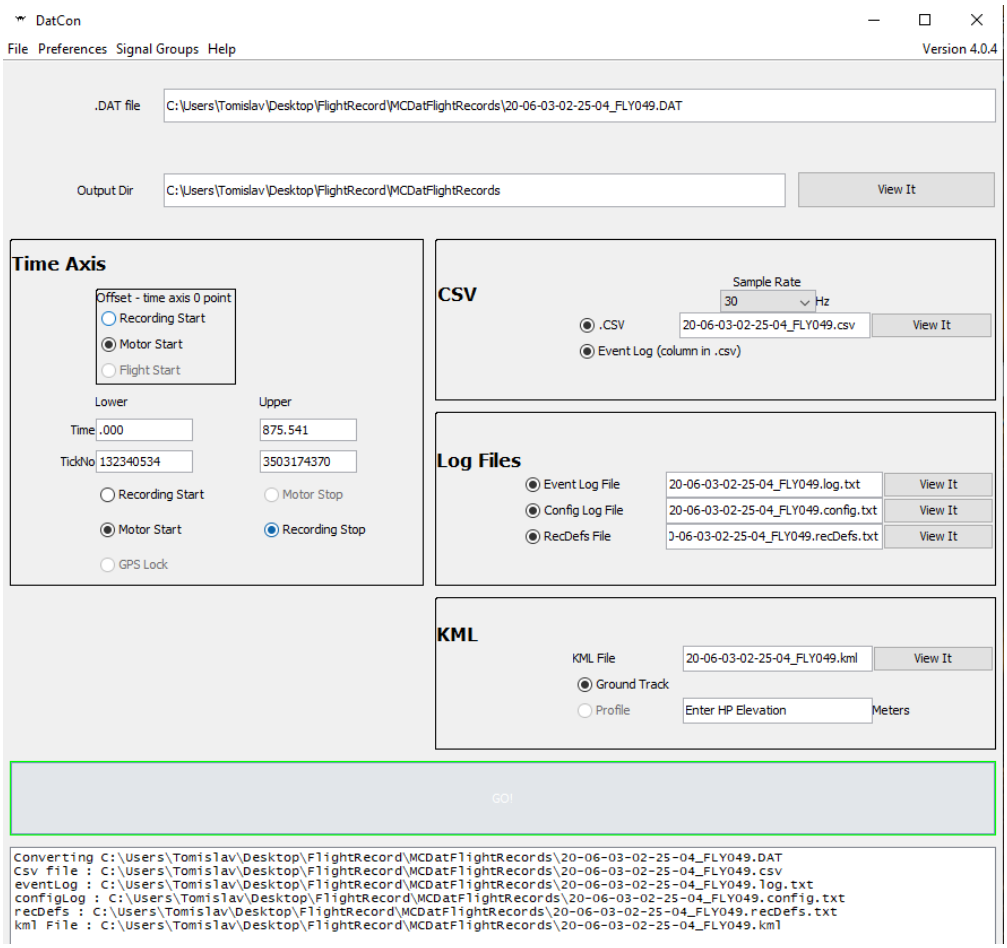
Njegovim pregledom, može se utvrditi kako se kreira za vrijeme prepoznavanja i prilagodbe formata vanjske SD memorije bespilotnog zrakoplova prema mobilnom uređaju. U njemu su vidljivi podaci o korištenom uređaju te o *e-mail* računu vezanom uz DJI korisnički račun.

Slika 15. Prikaz *debug_log* zapisa

Nadalje, u direktoriju mape „DJI“ moguće je pronaći različite *log* zapise vezane za *cache* memoriju ali s obzirom na to kako su enkodirani, ne može ih se s lakoćom interpretirati. Uz to, moguće je pronaći fotografije, videozapise s uputama za letenje te glazbu korištenu u aplikaciji video uređivača dostupnoj unutar DJI GO 4 aplikacije.

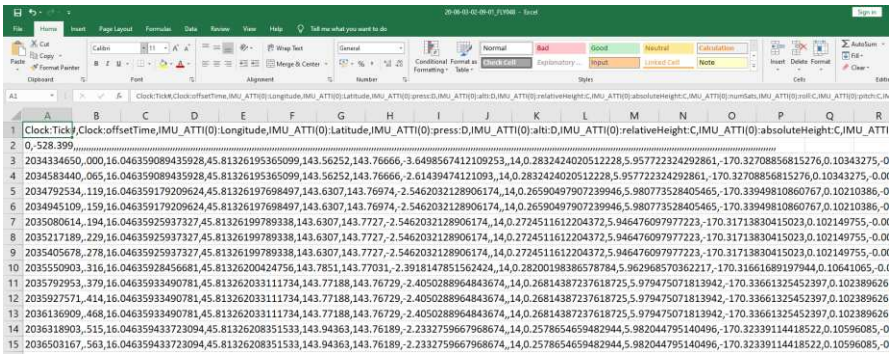
Podatke svakog pojedinog leta moguće je pronaći u mapi „*FlightRecord*“ koja kao što joj i ime glasi, sadrži *log* zapise u .DAT formatu datoteka. Prema [50], odnoseći se pritom na model DJI Mavic Air, .DAT datoteke dohvaćene s unutarnje pohrane bespilotnog zrakoplova su kriptirane te im nije moguće pristupiti dok datoteke istog formata dohvaćene s direktorija letačke aplikacije na mobilnom uređaju mogu biti procesirane.

Njihova interpretacija vrši se programima DatCon i CsvView koje je potrebno preuzeti na forenzičku radnu stanicu. Prvo se koristi DatCon koji .DAT format pretvara u formate pogodne za daljnju analizu na programima i uslugama poput CsvView, Excel te Google Earth.



Slika 16. Prikaz sučelja i mogućnosti DatCon programa

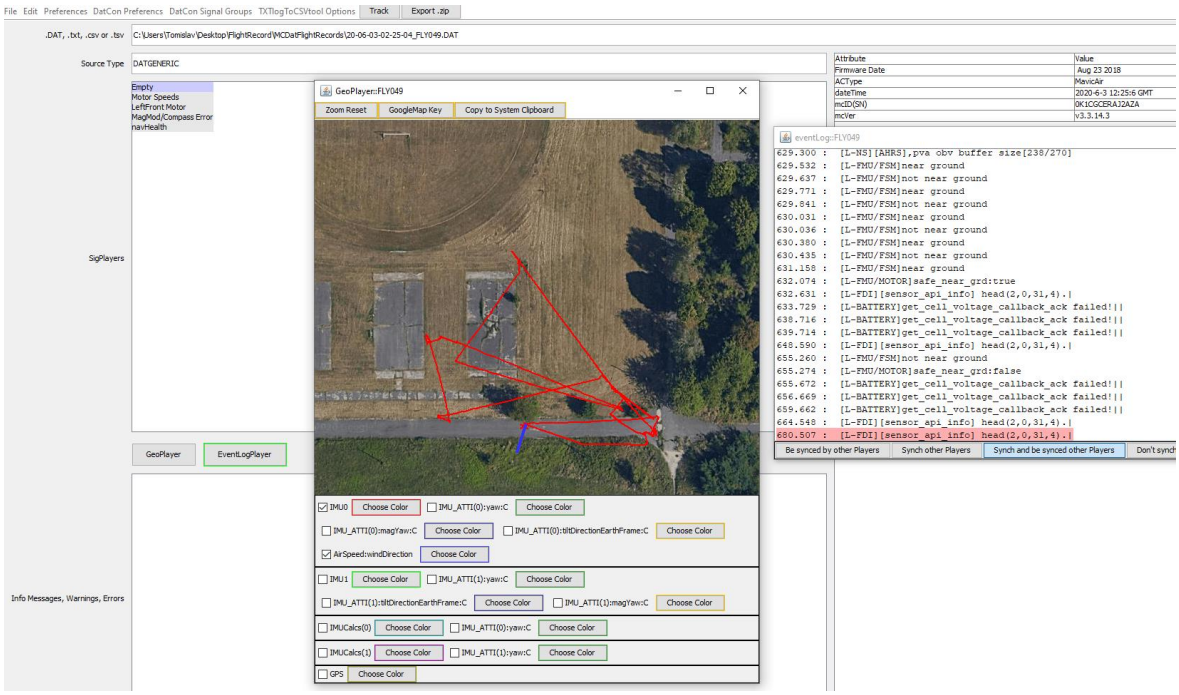
Nakon spomenute konverzije, cijeli *log* zapis leta moguće je otvoriti unutar Excel programa gdje su sve vrijednosti prikazane u .CSV formatu (tekstualni format gdje su podaci odvojeni razdjelnim znakom). Podaci se sastoje od vremena polijetanja, geografske dužine i širine, relativne/apsolutne visine, stanja baterijskih ćelija, smjeru dolaznog vjetra, datuma i sl. te kao takvi nisu pogodni za vizualnu interpretaciju.



Slika 17. Prikaz podataka iz .CSV datoteke

CsvView program može otvoriti kreiranu .CSV datoteku koju zatim, uz pomoć GoogleEarth API-a, vizualno prikaže kao putanju na satelitskom prikazu lokacije letačkih aktivnosti. Dodatno su prikazani podaci poput smjera vjetra (plava crta) te detaljnog tehničkog *log* zapisa kojeg je teško interpretirati bez stručnijeg znanja o principu rada bespilotnog zrakoplova (slika 18).

Kombinacijom ovih alata moguće je prikazati točnu putanju leta, geolokacijske podatke, pronaći *e-mail* adresu kojom je registrirana letačka aplikacija te ostale senzorske podatke usko vezane uz sam let čime se mogu saznati ključni detalji istrage.



Slika 18. Vizualni prikaz leta i *log* zapis unutar CsvView programa

Prema [51], tvrtka DJI tvornički je omogućila dodatno obogaćivanje snimljenih fotografija putem širokog spektra metapodataka. Oni u samom formatu .JPG nisu vidljivi već se nalaze unutar same slike. Podaci poput vremenski oznaka, GPS informacija, visine, geografske širine i dužine i sl. povezani su putem datoteke formata .EXIF.

Dodatno, isti izvor navodi kako se podaci o vremenu na letačkoj aplikaciji DJI GO 4 sinkroniziraju s lokalnim vremenom na uređaju pa je hipotetski moguće izmijeniti vrijeme ili vremensku zonu na mobilnom uređaju kako bi se izmijenili zapisani podaci nad letačkom aplikacijom (odstupanje od stvarnog vremena). Takve detalje pažljiv forenzički istražitelj treba imati u cilju što prije saznati.

6.3.2. Analiza podataka dohvaćenih Cellebrite UFED Touch 2

DJI Mavic Air – Datotečna ekstrakcija

Kao što je prethodno rečeno za DJI Mavic Air izvršene su dvije ekstrakcije, datotečna te fizička. Obje će biti opisane u nastavku.

Summary

UFED Physical Analyzer version	7.33.0.30
Report creation time	6/10/2020 10:20:03 AM +02:00
Time zone settings (UTC)	Original UTC value
Examiner name	Tomislav Kletuš
Location	Borongajska cesta 83f, 10000 Zagreb
Case number	1
Case name	DJI Mavic Air
Department	Laboratorij za sigurnost i forenzičku analizu informacijsko-komunikacijskog sustava
Organization	Zavod za informacijsko-komunikacijski promet

Source Extraction

File System	
Extraction start date/time	6/4/2020 10:48:47 AM(UTC+2)
Extraction end date/time	6/4/2020 11:07:14 AM(UTC+2)
Unit identifier	7211345
UFED version	7.33.0.95
Internal version	7.33.0.95
Selected manufacturer	Drone
Selected device name	DJI - Mavic Air
Machine name	TOUCH2-7211345
Connection type	Cable No. 170
Extraction type	File System
Extraction ID	81A11445-9AE2-4E04-9AF0-C4C4E4FC002C
Extraction (UFD) file data integrity	Intact

Slika 19. Pregled osnovnih informacija o datotečnoj ekstrakciji

Osnovne informacije (tko je proveo ekstrakciju, putem kojeg uređaja i nad kojim uređajem, vrijeme/datum, mjesto, metoda ekstrakcije te status integriteta podatka) o datotečnoj ekstrakciji, kreirane kroz izvješće nakon završetka iste, analizirane su UFED Reader alatom.

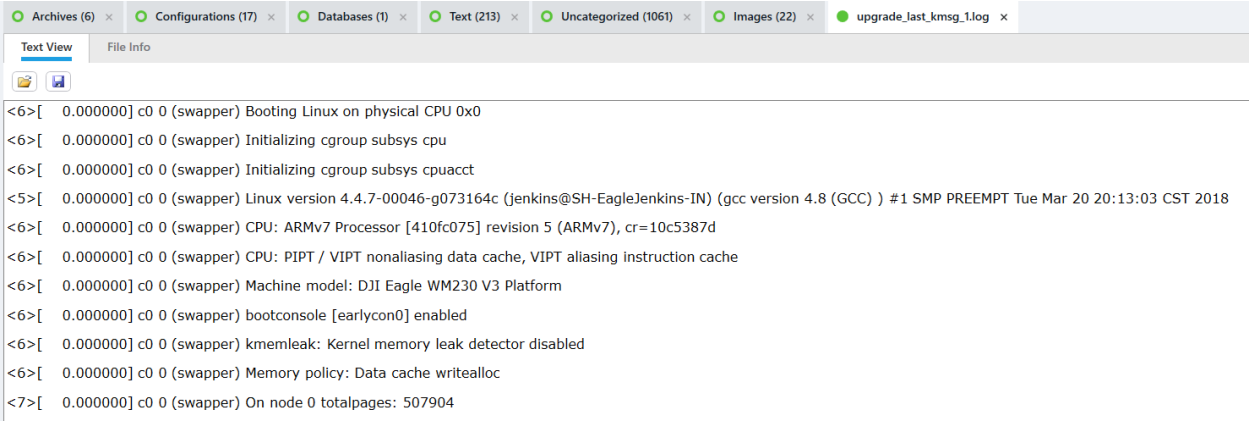
Obujam dohvaćenih kategoriziranih podataka datotečnom ekstrakcijom je sljedeći:

1. Data Files (1298)
    - Archives (6)
    - Configurations (17)
    - Uncategorized (1061)
    - Databases (1)
    - Text (213)

2. Media (22)
    - Images (22)

Arhivski podaci i konfiguracijske datoteke su većinom prazni podaci bez ikakvog sadržaja osim imena, putanje i veličine. Prema imenu može se zaključiti kako je kod arhivskih podataka riječ o određenim *recovery* datotekama dok se konfiguracijski podaci odnose na interne postavke senzora kamere, FTP (engl. *File Transfer Protocol*) protokola, Wi-Fi mreže, testnih skripti i sl. Nekategoriziranih podataka kvantitativno ima najviše, raznih su formata i ekstenzija ali također ne sadrže nikakve interpretativne podatke osim imena, veličine i putanje od kuda su dohvaćene.

Kroz ovaj tip ekstrakcije dohvaćena je jedna baza podataka imena dynamic.db koja je ujedno i prazna. Unutar tekstualne kategorije, većinom su dohvaćeni *log* zapisi vezani uz aktivnosti senzora s bespilotnog zrakoplova. Iste je veoma teško interpretirati bez većeg tehničkog znanja. Zanimljivo je kako se unutar tih zapisa može doći do informacije o tome da je DJI operativni sustav na kontroloru leta temeljen na nekoj verziji Linux OS-a.



Slika 20. Primjer dohvaćenog tekstualnog, *log* podataka

Također, od multimedijskih datoteka dohvaćene su tzv. *built-in* prikazi sistemskih ikona i sl. Ukupno je jedanaest slika te su sve dohvaćene kao duplicirane.

<u>DJI Mavic Air – Fizička ekstrakcija</u>

Analogno osnovnim informacija iz izvješća datotečne ekstrakcije i za fizičku ekstrakciju dostupne su osnovne informacije fizičke ekstrakcije. Ovo izvješće sastoji se od ukupno 8 stranica te sadrži vrlo slične ili identične stavke. Jedina razlika je vrlo gruba točkasto određena lokacija gdje su dohvaćene datoteke kreirane.

Extraction Report - Drone DJI - Mavic Air

Cellebrite
www.cellebrite.com

Summary

UFED Physical Analyzer version	7.33.0.30
Report creation time	6/10/2020 11:09:01 AM +02:00
Time zone settings (UTC)	Original UTC value
Translated languages	
Examiner name	Tomislav Kletuš
Location	Borongajska cesta 83f, 10000 Zagreb
Case number	1
Case name	DJI Mavic Air
Department	Laboratorij za sigurnost i forenzičku analizu informacijsko-komunikacijskog sustava
Organization	Zavod za informacijsko-komunikacijski promet

Source Extraction

Physical	
Extraction start date/time	6/4/2020 9:43:40 AM(UTC+2)
Extraction end date/time	6/4/2020 10:36:44 AM(UTC+2)
Unit identifier	7211345
UFED version	7.33.0.95
Internal version	7.33.0.95
Selected manufacturer	Drone
Selected device name	DJI - Mavic Air
Machine name	TOUCH2-7211345
Connection type	Cable No. 170
Extraction type	Physical
Extraction ID	7A606259-FD09-4331-B3C6-6DE4BD710570
Extraction (UFD) file data integrity	Intact

Slika 21. Pregled osnovnih informacija o fizičkoj ekstrakciji

Prilikom ekstrakcije svi dohvaćeni podatci su kategorizirani radi lakšeg snalaženja tijekom analize. Obujam dohvaćenih kategoriziranih podataka fizičkom ekstrakcijom je sljedeći:

1. Data Files (15) (5)
    - Uncategorized (15) (5) (x) = broj dohvaćenih obrisanih podataka
2. Location Related (6)
    - Device Locations (6)
3. Media (18)
    - Images (12)
    - Videos (6)

Unutar nekategoriziranih podataka moguće je pronaći različite podatke poput formata .GIS, .SRT koji su prethodno opisani a unutar ove forenzičke metode nisu prepoznati kao geolokacijski ili kao tekstualni. Uz njih, ovdje je moguće isključivo vidjeti obrisane podatke uz informacije o imenu, putanji direktorija te datumu i vremenu njihova kreiranja. Među tih 5 obrisanih datoteka, prema njihovim formatima te putanji direktorija moguće je odrediti koje su vrste.

Prva datoteka imena je *.DJI_0032.MP4.avc1*, putanje *NO NAME/DCIM/100MEDIA/.DJI_0032.MP4.avc1* te je dodatno opisana vremenom kreiranja „3.6.2020. 14:47:18“. Polje *Deleted time* nije popunjeno te nema informacije o trenutku brisanja.

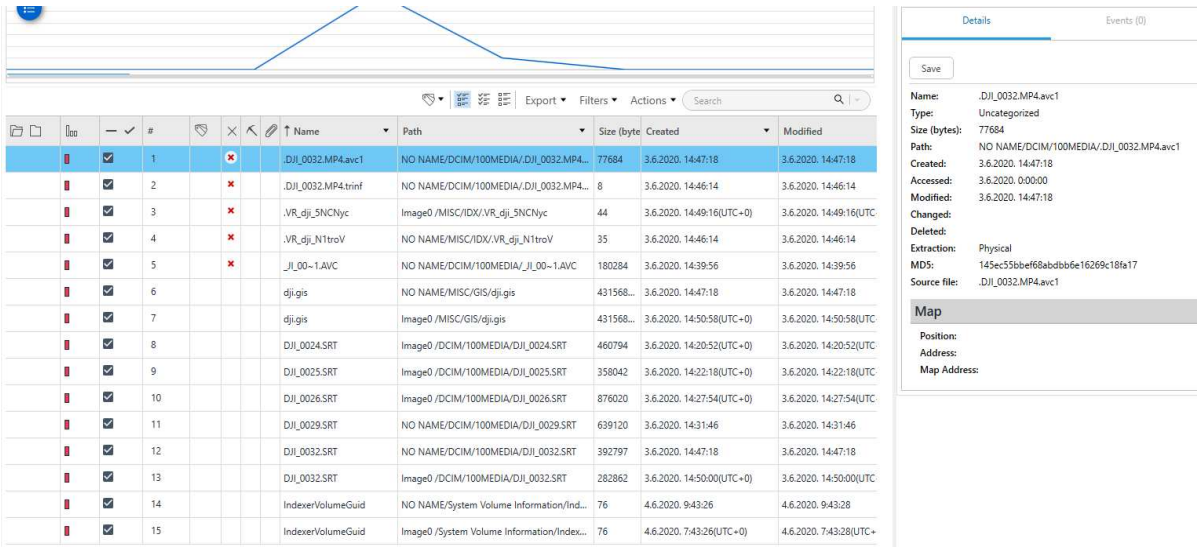
Iz navedenog, može se zaključiti da je ta datoteka u stvari videozapis. S obzirom da se prema scenariju u 14:45h započelo s brisanjem jednog videozapise i jedne fotografije s oba tipa pohrane, onda informacija o vremenu kreiranja zapravo označava vrijeme brisanja. Jedini problem je što se jednoznačno ne može odrediti na kojem tipu pohrane se nalazio podatak. Razlog tome je što se na obje multimedijske datoteke spremaju na identičnu putanju. Za drugu datoteku vrijedi sve ovdje navedeno.

Treća datoteka imena je *.VR_dji_5NCNyc*, putanje *Image0 /MISC/IDX/.VR_dji_5NCNyc* gdje također za nju postoji vrijeme i datum kreiranja „3.6.2020. 14:49:16(UTC+0)“. Prema imenu nije moguće odrediti što datoteka predstavlja jer nema prepoznatljivog imena (DJIxxxx.format) niti ekstenzije datoteke.

Jedino se prema putanji može pretpostaviti kako je riječ o slici tj. fotografiji te njeno vrijeme kreiranja ulazi u vrijeme brisanja datoteka sukladno početnom scenariju. Također, niti kod ove datoteke ne može se sa sigurnošću reći na kojem tipu pohrane se nalazila. Zanimljiva je činjenica ako se pretpostavi kako je riječ o fotografiji, njena putanja ne odgovara putanji gdje DJI Mavic Air pohranjuje snimljene fotografije *DCIM/100MEDIA.* Za četvrtu datoteku vrijedi sve ovdje navedeno.

Peta datoteka, imena *_JI_00~1.AVC* malo odskače od ostalih jer je prema oznaci vremena kreirana „3.6.2020. 14:39:56“, što izlazi iz okvira kada su se dogodila brisanja podataka.

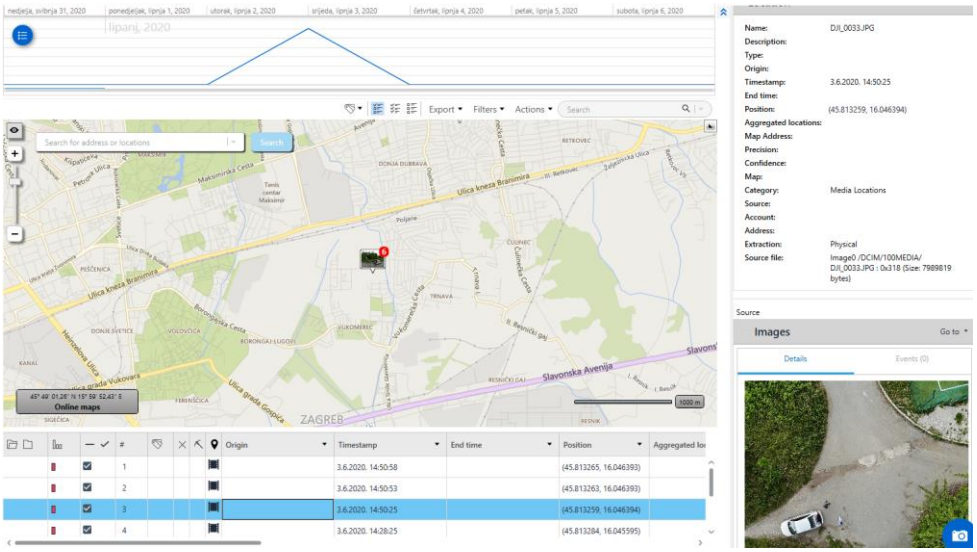
Mogućnost automatskog brisanja prema nekim tvorničkim mehanizmima nije isključena ali putanja *NO NAME/DCIM/100MEDIA/_JI_00~1.AVC* ukazuje kako je riječ o videozapisu s formatom .AVC (engl. *Advanced Video Coding*). Nije isključena slučajno okidanje procesa brisanja od strane pilota na daljinu kod izvođenja letačkih aktivnosti.



Slika 22. Dohvaćeni nekategorizirani i obrisani podaci

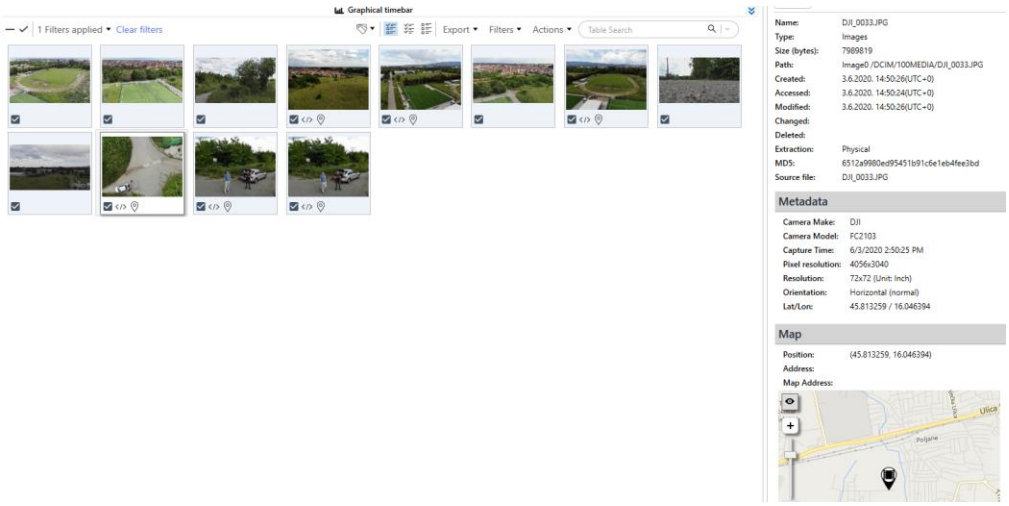
U skupu podataka povezanih s informacijom o lokaciji (*Location Related*) moguće je pregledati metapodatke za 6 dohvaćenih videozapisa.

Razlika kategorije *Device Locations* te kategorije *Videos* je što u ovoj posljednjoj uz datum i vrijeme kreiranja, ime i putanju nema podataka o geolokaciji na kojoj je videozapis snimljen. Moguće ih je otvoriti i pregledati u izvornom obliku videozapisa.



Slika 23. Prikaz dohvaćene lokacije videozapisa

Unutar kategorije snimljenih fotografija dohvaćeno je ukupno 12 datoteka. U tom skupu datoteka nalaze se one s već spomenutim formatom .THM te .JPG. Svaka fotografija ima prikaz svoje putanje, imena, veličine te datuma i vremena kreiranja. Uz svaku dohvaćenu .JPG datoteku postoji informacija o geografskim koordinatama gdje je snimljena te su one obogaćene dodatnim podacima u .EXIF ekstenziji.



Slika 24. Prikaz dohvaćenih fotografija i dodatnih podataka

Popis metapodataka dodanih .EXIF datotekom je jako velik, istom se može pristupiti nakon otvaranja pojedinosti o svakoj fotografiji zasebno. Uz konfiguracijske informacije o senzoru kamere, informacije o lokaciji, kontrastu, saturaciji, oštrini, rezoluciji i ostalim sličnim podacima, zanimljiva činjenica je kako se unutar seta .EXIF podataka može pronaći i visina na kojoj je fotografija snimljena.

EXIF	
GPSVersionID	Byte[] Array
GPSLatitudeRef	N
GPSLatitude	45, 48, 47.7348986857143
GPSLongitudeRef	E
GPSLongitude	16, 2, 47.0191309857143
GPSAltitudeRef	0
GPSAltitude	17.5
ImageDescription	created by dji camera
Make	DJI
Model	FC2103
Orientation	1
XResolution	72
YResolution	72
ResolutionUnit	2
Software	10.00.14.05
DateTime	2020:06:03 14:50:25
YCbCrPositioning	1
ExposureTime	0.00570671
FNumber	2.8
ExposureProgram	2
ISOSpeedRatings	108
ExifVersion	2814302915, 3953358179, 4009292833, 901225478
DateTimeOriginal	2020:06:03 14:50:25
DateTimeDigitized	2020:06:03 14:50:25
ComponentsConfiguration	8834, 131075, 2, 69
CompressedBitsPerPixel	4.61737192463407
ApertureValue	2.971
ExposureBiasValue	0
MaxApertureValue	2.971
SubjectDistance	NaN
MeteringMode	1
LightSource	0
Flash	32
FocalLength	4.5
FlashpixVersion	1036502034, 3032586961, 3371461864, 1226001454
ColorSpace	1
PixelXDimension	4056
PixelYDimension	3040
ExposureIndex	0.25
FileSource	3
SceneType	1
CustomRendered	0
ExposureMode	0
WhiteBalance	0
DigitalZoomRatio	NaN
FocalLengthIn35mmFilm	24
SceneCaptureType	0

Slika 25. Popis dohvaćenih metapodataka iz .EXIF datoteke

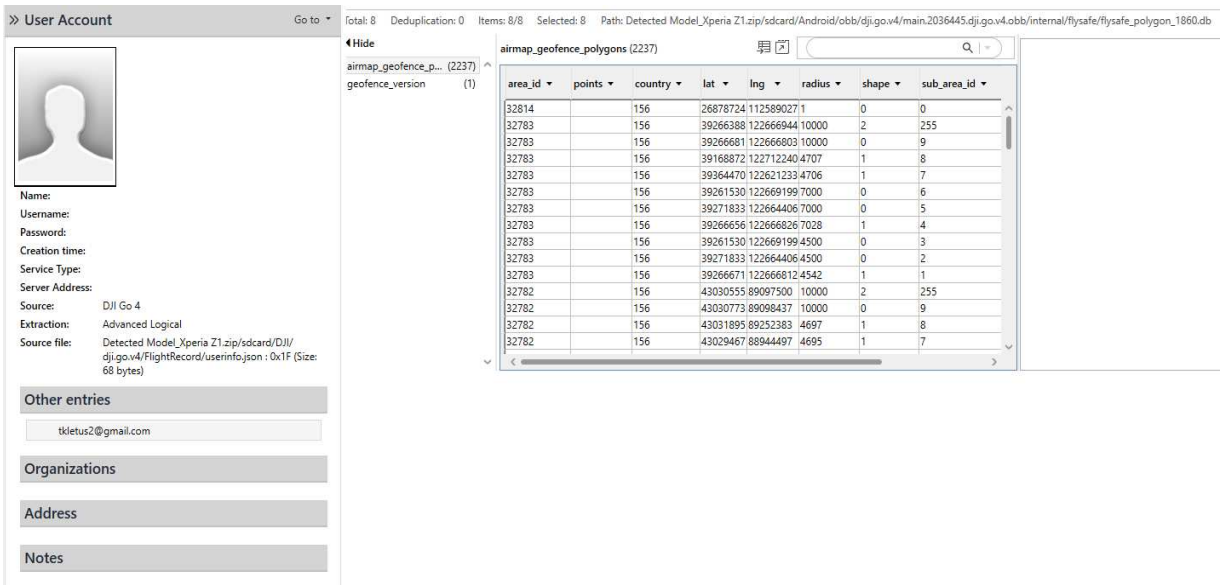
Sony Xperia Z1 – Napredna logička ekstrakcija i datotečna ekstrakcija

Nakon analize podataka napredne logičke ekstrakcije te također datotečne za navedeni mobilni uređaj, može se zaključiti kako je set dohvaćenih podataka između bespilotnog zrakoplova te mobilnog uređaja, odnosno letačke aplikacija vrlo sličan, a u nekim instancama i identičan. Naime, putem ove metode dohvaćena je cijela logička i datotečna slika uređaja unutar kojih je bilo potrebno potražiti podatke vezane uz DJI GO 4 aplikaciju, najčešće pregledom putanje direktorija.

Ovim metodama pronađeni su identični podaci kao i kod ručne ekstrakcije poput ugrađene DJI glazbe, ugrađenih DJI fotografija, snimljenih fotografija i videozapisa. Također su pronađeni identični *log* zapisi kao i GPS koordinate na kojima su se vršile letačke aktivnosti i aktivnosti snimanja iz zraka.

Neki od dokaza koji su jedinstveno dohvaćeni ovim metodama su točna e-mail adresa s putanjom na DJI GO 4 aplikaciju čime se može otkriti tko je koristio istu i povezujući je s GPS podacima zaključiti gdje ju je koristio. Drugi tip podataka koji je jedinstveno dohvaćen ovim metodama je baza podataka.

Prema podacima smještenim u bazi podataka poput ID-a područja, njegovog radijusa, geografske širine i dužine te visine pružaju pretpostavku o DJI tvorničkoj bazi koja unutar aplikacije ograničava letačke aktivnosti nad visoko rizičnim područjima poput zračnih luka i ostalih područja vezana uz sigurnost pojedinca ili državnog interesa.



Slika 26. Prikaz baze podataka za letna ograničenja

Glavna razlika između napredne logičke i datotečne ekstrakcije, koja je uočena tijekom provođenja analize, je što napredna logička ne dohvaća tzv. *thumbnail* slike, tj. datoteke s .THM ekstenzijom te ne dohvaća metapodatke unutar .EXIF ekstenzije za .JPG fotografije.

Također, uočeno je kako se prilikom datotečne ekstrakcije dohvate .EXIF metapodaci ali isključivo za tvorničke DJI fotografije, ne i za snimljene fotografije. Iz tog razloga, kod analize podataka obiju metoda, nije moguće pronaći GPS podatke povezne izravno na snimljenu fotografiju ili videozapis.

7. Zaključak

Razvojem bespilotnih zrakoplova te njihovim približavanjem širem spektru potencijalnih korisnika snižavanjem cijene, isti su postali vrlo popularni zadnjih nekoliko godina za korištenje u civilne namijene. Osim što su donijeli napredak i proširili vidike moguće primjene unutar područja poput poljoprivrede, edukacije te ostalih privrednih i znanstvenih djelatnosti, postali su i pomoćna sredstva za kriminalne aktivnosti. Sposobnost nošenja različitih oblika opreme pa tako i vojnih, u sigurnosnom smislu predstavlja prijetnju jer u ne željenim rukama mogu prouzročiti veliku materijalnu štetu ili čak ljudske žrtve.

Iz navedenih razloga bespilotni zrakoplovi postaju zanimljivi forenzičkim istražiteljima i stručnjacima koji se trude biti korak ispred kriminalaca te bespilotne zrakoplova iz incidentnih situacija forenzički ispitati te donijeti zaključke koji bi bili korisni u sudskim postupcima. Nadalje, kako je digitalna forenzika bespilotnih zrakoplova, nova znanstvena disciplina, ne postojanje i nedostatak adekvatnih pravnih akata i standardizirane procedure predstavlja problem i stvara poteškoće forenzičkim stručnjacima u njihovom radu. Širenjem spoznaja o bespilotnim zrakoplovima i njihovoj forenzičkoj proceduri trebalo bi rezultirati donošenjem adekvatne standardizacije i zakonodavnog okvira u budućnosti.

U ovom diplomskom radu prikazan je postupak forenzičke istrage komercijalnog bespilotnog zrakoplova i njemu ključnih povezanih elemenata, od ekstrakcije podataka do njihove analize. U prva četiri poglavlja, dan je osvrt na bespilotne zrakoplove kao novi rastući tehnološki trend koji spaja mogućnosti mobilnih terminalnih uređaja s principima zrakoplovstva uz prikaz mogućnosti zlouporabe te njima suprotnih sigurnosnih mjera. Količina dohvaćenih podataka te mogućnosti ekstrakcije ovise o više faktora poput karakteristika i modela bespilotnog zrakoplova, korištene letačke aplikacije pridružene mobilnom telefonu te na kraju mogućnosti dostupnih forenzičkih alata. Preciznije, metode enkripcije koje operativni sustavi mobilnih uređaja i bespilotnih zrakoplova vrše nad setom podataka, igraju ključnu ulogu u kompleksnosti ekstrakcije i kasnijoj interpretaciji istih.

Nakon izvršene analize, rezultat istraživanja ovog diplomskog rada je kako za bespilotni zrakoplov tvrtke DJI nije dovoljno imati jedan od kvalitetnijih forenzičkih alata poput UFED Touch 2. Razlog tomu je nemogućnost dohvaćanja većeg spektra podataka s mobilnih uređaja uz prilagođene verzije OS-a te nemogućnost interpretacije ekstrahiranih obrisanih podataka. Pomoćni alati specijalizirane namjene poput CscView, istražiteljima mogu vizualno bolje približiti putanje leta i sl. podatke. U konačnici je vidljivo kako sama forenzička istraga bespilotnih zrakoplova zahtjeva puno vremena, testiranje mogućnosti forenzičkih alata te prethodnog tehnološkog znanja. Tek kombinacijom korištenja različitih naprednih i manje naprednih alata uz višestruke metode ekstrakcije, raste vjerojatnost dohvata i interpretacije digitalnih dokaza.

Popis literature

[1] Besada, J. A., Bernardos, A. M., Bergesio, L., Vaquero, D., Campana, I., & Casar, J. R. (2019): *Drones-as-a-service: A management architecture to provide mission planning, resource brokerage and operation support for fleets of drones*. 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Madrid: Universidad Politécnica de Madrid; 2019. Preuzeto sa: https://ieeexplore.ieee.org/document/8730838 [Pristupljeno: travanj 2020.]

[2] Maune, K. G.: *A Forensic Analysis of the Parot AR Drone 2.0.* University of Derby, Department of Electronics, Computing and Mathematics; 2018. Preuzeto sa: https://computing.derby.ac.uk/c/wp-content/uploads/2018/09/A-Forensic-Analysis-of-the-Parrot-AR-Drone-2.0..pdf [Pristupljeno: travanj 2020.]

[3] Jetmash: 4 Types of drones you should know. Preuzeto sa: https://jetmash.com/types-of-drones-you-should-know [Pristupljeno: travanj 2020.]

[4] Grind Drone: Drone Components_Quick List of it's Parts. Preuzeto sa: http://grinddrone.com/drone-features/drone-components [Pristupljeno: svibanj 2020.]

[5] SensorsOnline: Technology That Makes Drones Work. Preuzeto sa: https://www.fierceelectronics.com/components/how-many-sensors-are-a-drone-and-what-do-they-do [Pristupljeno: svibanj 2020.]

[6] CCAA - Hrvatska agencija za civilno zrakoplovstvo. *Zahtjevi za operatora za izvođenje letačkih operacija sustavima bespilotnih zrakoplova.* Preuzeto sa: http://www.ccaa.hr/upload/files/documents/Zahtjevi%20za%20operatora%20za%20izvo%C4%91enje%20leta%C4%8Dkih%20operacija%20sustavima%20bespilotnih%20zrakoplova.pdf [Pristupljeno: svibanj 2020.]

[7] Jain, U., Rogers, M., & Matson, E. T.: *Drone forensic framework: Sensor and data identification and verification*. 2017 IEEE Sensors Applications Symposium (SAS). Indiana, USA: Purdue University; 2017. Preuzeto sa: https://ieeexplore.ieee.org/document/7894059 [Pristupljeno: svibanj 2020.]

[8] Valavanis K. P., Vachtsevanos G. J.: *Handbook of Unmanned Aerial Vehicles*, Springer Netherland, 2015. Preuzeto sa: https://link.springer.com/referencework/10.1007%2F978-90-481-9707-1 [Pristupljeno: svibanj 2020.]

[9] SensorsOnline: Technology That Makes Drones Work. Preuzeto sa: https://www.sensorsmag.com/components/how-many-sensors-are-a-drone-and-what-do-they-do. [Pristupljeno: svibanj 2020.]

[10] How do drones work? IMU – Inertial Measurement Unit. Preuzeto sa: https://www.linkedin.com/pulse/how-do-drones-work-part-9-imu-inertial-measurement-unit-fiorenzani. [Pristupljeno: svibanj 2020.]

[11] AZO Sensors: How do Tilt Sensors Work. Preuzeto sa: https://www.azosensors.com/article.aspx?ArticleID=318. [Pristupljeno: svibanj 2020.]

[12] Regimage.org: Drone Parts. Preuzeto sa: http://www.regimage.org/drone-parts/ [Pristupljeno: rujan 2020.]

[13] DJIcdn: DJI Ground Station Product Release Notes. Preuzeto sa: http://dl.djicdn.com/downloads/groundstation/en/Ground_Station_release_notes_en.pdf [Pristupljeno: svibanj 2020.]

[14] ArduPilot: Choosing a Ground Station. Preuzeto sa: https://ardupilot.org/copter/docs/common-choosing-a-ground-station.html [Pristupljeno: svibanj 2020.]

[15] BlackSwiftTechnologies: SwiftCore Flight Management System. Preuzeto sa: https://bst.aero/swiftcore-flight-management-system/ [Pristupljeno: svibanj 2020.]

[16] Kittyhawk.io: Kittyhawk Air Control. Preuzeto sa: https://kittyhawk.io/air-control/ [Pristupljeno: svibanj 2020.]

[17] Sans.org: Kovar, D.: UAV (aka drone) Forensics. Preuzeto sa: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492184184.pdf [Pristupljeno: svibanj 2020.]

[18] DJI.com.: Mavic Air Specs. Preuzeto sa: https://www.dji.com/hr/mavic-air/info#specs [Pristupljeno: svibanj 2020.]

[19] Portal *StyleAndEasyMagazine*. Preuzeto sa: https://styleandeasy.com/2018/04/08/dji-mavic-air-the-best-of-dji-spark-and-mavic-pro-in-one-device/ [Pristupljeno: svibanj 2020.]

[20] Zdnet: How drone forensics can reveal pilot identity. Preuzeto sa: https://www.zdnet.com/article/how-drone-forensics-can-reveal-pilot-identity/ [Pristupljeno: svibanj 2020.]

[21] Digitpol.com.: Drone Forensic Investigation. Preuzeto sa: https://digitpol.com/drone-forensics/ [Pristupljeno: svibanj 2020.]

[22] Watson, S.: *Drone Forensics An update on a U.S. Department of Homeland Security R&D Project*. VTO Labs. Preuzeto sa: https://dfrws.org/sites/default/files/session-files/pres_drone_forensics_program.pdf [Pristupljeno: svibanj 2020.]

[23] Azhar, M A Hannan Bin & Barton, Thomas & Islam, Tasmina: Drone *Forensic Analysis Using Open Source Tools in The Journal of Digital Forensics, Security and Law*. Canterbury: Computing, Digital Forensics and Cybersecurity Canterbury Christ Church University; 2018. Preuzeto sa: https://www.researchgate.net/publication/324994744_Drone_Forensic_Analysis_Using_Open_Source_Tools_in_The_Journal_of_Digital_Forensics_Security_and_Law [Pristupljeno: svibanj 2020.]

[24] Renduchintala, A. L. P. S., Albehadili, A., & Javaid, A. Y.: *Drone Forensics: Digital Flight Log Examination Framework for Micro Drones*. 2017 International Conference on Computational Science and Computational Intelligence (CSCI). Toledo: University of Toledo; 2017. Preuzeto sa: https://ieeexplore.ieee.org/document/8560767 [Pristupljeno: svibanj 2020.]

[25] Narodne Novine. *Pravilnik o sustavima bespilotnih zrakoplova*. Preuzeto sa: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_11_104_2040.html [Pristupljeno: svibanj 2020.]

[26] CCAA - Hrvatska agencija za civilno zrakoplovstvo. *Informacije o kategorijama*. Preuzeto sa: https://drone.ccaa.hr/user/index.php# [Pristupljeno: svibanj 2020.]

[27] CCAA - Hrvatska agencija za civilno zrakoplovstvo. *Zahtjevi za operatora za izvođenje letačkih operacija sustavima bespilotnih zrakoplova.* Preuzeto sa*:* http://www.ccaa.hr/upload/files/documents/Zahtjevi%20za%20operatora%20za%20izvo%C4%91enje%20leta%C4%8Dkih%20operacija%20sustavima%20bespilotnih%20zrakoplova.pdf [Pristupljeno: svibanj 2020.]

[28] Narodne Novine. *Uredba o snimanju iz zraka*. Preuzeto sa: https://narodne-novine.nn.hr/clanci/sluzbeni/2019_03_28_572.html [Pristupljeno: svibanj 2020.]

[29] DroneRules.eu: zaštita privatnih podataka za rekreativce. Preuzeto sa: https://dronerules.eu/hr/recreational/obligations/summary-of-privacy-rules-in-eu-1 [Pristupljeno: svibanj 2020.]

[30] Poslovni.hr: U Hrvatskoj oko 2200 operatora dronova. Preuzeto sa: http://www.poslovni.hr/hrvatska/u-hrvatskoj-oko-2200-operatora-dronova-354703 [Pristupljeno: svibanj 2020.]

[31] Business Insider: *Exploring the latest drone technology for commercial, industrial and military drone uses*. Preuzeto sa: https://www.businessinsider.com/drone-technology-uses-2017-7 [Pristupljeno: svibanj 2020.]

[32] Secretary of State for the Home Department by Command of Her Majesty: *UK Counter-Unmanned Aircraft Strategy*; 2019. Preuzeto sa: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840789/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf [Pristupljeno: svibanj 2020.]

[33] Dey, V., Pudi, V., Chattopadhyay, A., & Elovici, Y. (2018): *Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study*. 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID). Preuzeto sa: https://ieeexplore.ieee.org/document/8326960 [Pristupljeno: svibanj 2020.]

[34] Eriksson, N. (2018): *Conceptual study of a future drone detection system*. Department of Industrial and Materials Science, Chalmers University of Technology; Gothenburg, Sweden 2018. Preuzeto sa: http://publications.lib.chalmers.se/records/fulltext/255103/255103.pdf [Pristupljeno: svibanj 2020.]

[35] EDRMagazine.eu: Raytheon: C-UAS capabilities move to the next level. Preuzeto sa: https://www.edrmagazine.eu/raytheon-c-uas-capabilities-move-to-the-next-level [Pristupljeno: svibanj 2020.]

[36] Bouafif, H., Kamoun, F., Iqbal, F., & Marrington, A.: *Drone Forensics: Challenges and New Insights*. 2018 9th IFIP International Conference on New Technologies, Mobility and Security. Tunis, UAE: ESPRIT School of Engineering and Zayed University, College of Technical Innovation; 2018. Preuzeto sa: https://ieeexplore.ieee.org/document/8328747 [Pristupljeno: kolovoz 2020.]

[37] Azhar, H.: *Challenges and Techniques in Drone Forensics,* Canterbury Christ Church University; 2019. Preuzeto sa: http://www.iaria.org/conferences2019/filesCYBER19/HannanAzhar_Tutorial_ChallengesAndTechniques.pdf [Pristupljeno: kolovoz 2020.]

[38] Murphy, A. C.: *Developing Process for Mobile Device Forensics*, SANS Institute; 2011. Preuzeto sa: https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf [Pristupljeno: kolovoz 2020.]

[39] Bommisetty, S., Tamma, R., Mahalik, H.: *Practical Mobile Forensics*, Birmingham, 2012. Preuzeto sa: https://pre-uneplive.unep.org/redesign/media/assets/images/Practical%20Mobile%20Forensics.pdf [Pristupljeno: kolovoz 2020.]

[40] Autorizirana predavanja: *Forenzička analiza informacijsko komunikacijskog sustava: Digitalni dokazi i ekstrakcija podataka mobilnih uređaja*, Fakultet prometnih znanosti. Preuzeto sa: https://moodle.srce.hr/2019-2020/pluginfile.php/3071563/mod_resource/content/2/06_Digitalni%20dokazi%20i%20ru%C4%8Dna%20ekstrakcija.pdf [Pristupljeno: kolovoz 2020.]

[41] Mobile Forensics Workshop and Webcast: *Mobile Device Forensics: A – Z*; NIST; 2014. Preuzeto sa: https://www.nist.gov/system/files/documents/forensics/2-Brothers-NIST-2014_Slides-23-Pages-2.pdf [Pristupljeno: kolovoz 2020.]

[42] Special Counsel: *3 Methods of Mobile Device Extractions and the Data Each Contains (2016.),* Preuzeto sa: https://blog.specialcounsel.com/ediscovery/three-types-of-mobile-device-extractions-and-what-each-contains/ [Pristupljeno: kolovoz 2020.]

[43] Autorizirana predavanja: Forenzička analiza informacijsko komunikacijskog sustava: Digitalni dokazi i ekstrakcija podataka mobilnih uređaja, Fakultet prometnih znanosti. Preuzeto sa: https://moodle.srce.hr/2019-2020/pluginfile.php/3311558/mod_resource/content/1/07_Logi%C4%8Dka%2C%20datote%C4%8Dna%20i%20fizi%C4%8Dka%20ekstrakcija.pdf [Pristupljeno: kolovoz 2020.]

[44] digitalforensics.com: Chip-off Technique in Mobile Forensic; Preuzeto sa: https://www.digitalforensics.com/blog/chip-off-technique-in-mobile-forensics/ [Pristupljeno: kolovoz 2020.]

[45] jaytaylor.com: JTAGing Mobile Phones; Preuzeto sa: https://jaytaylor.com/notes/node/1479150923000.html [Pristupljeno: kolovoz 2020.]

[46] Zareen, A., & Baig, S. (2010). Notice of Violation of IEEE Publication Principles Mobile Phone Forensics: Challenges, Analysis and Tools Classification. 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. Preuzeto sa: https://ieeexplore.ieee.org/abstract/document/5491956 [Pristupljeno: kolovoz 2020.]

[47] Cellebrite.com: Cellebrite introduces UFED Touch2 platform; Preuzeto sa: https://www.cellebrite.com/en/press/cellebrite-introduces-ufed-touch2-platform/ [Pristupljeno: kolovoz 2020.]

[48] Teeltech.com: mobile-device-forensic-tools; Preuzeto sa: https://teeltech.com/mobile-device-forensic-tools/cellebrite/ufed-touch-ultimate/ [Pristupljeno: kolovoz 2020.]

[49] XDA-developers.com: What is Magisk?; Preuzeto sa: https://www.xda-developers.com/what-is-magisk/ [Pristupljeno: kolovoz 2020.]

[50] datfile.net: CsvView/DatCon; Preuzeto sa: https://datfile.net/index.html [Pristupljeno: kolovoz 2020.]

[51] Yousef, M., & Iqbal, F. (2019). Drone Forensics: A Case Study on a DJI Mavic Air. 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). Preuzeto sa: https://ieeexplore.ieee.org/abstract/document/9035365 [Pristupljeno: kolovoz 2020.]

Popis kratica

API	*(Application Programming Interface)*	aplikacijsko programibilno sučelje
AVC	*(Advanced Video Coding)*	format datoteke
CCAA	*(Croatian Civil Aviation Agency)*	hrvatska agencija za civilno zrakoplovstvo
C-UAS	*(Counter-Unmanned Aerial System)*	protu-bespilotno zrakoplovni sustav
DIY	*(Do It Yourself)*	napravi samostalno
DNA	*(Deoxyribonucleic acid)*	deoksiribonukleinska kiselina
EASA	*(European Union Aviation Safety Agency)*	europska agencija za sigurnost civilnog zrakoplovstva
eMMC	*(Embedded Multi-Media Controller)*	modul memorije i memorijskog kontrolera na mobilnom uređaju
ESC	*(Electronic Speed Controllers)*	kontroleri brzine
ESN	*(Electronic Serial Number)*	identifikacijski broj kojeg proizvođači ugrađuju u mikročip mobilnih uređaja
EXIF	*(Exchangeable Image File Format)*	format datoteke
FAT32	*(File Allocation Table)*	format arhitekture pohrane podataka
FMS	*(Flight Management Software)*	softver za upravljanje letom
FPV	*(First Person View)*	pogled iz prvog lica
FTP	*(File Transfer Protocol)*	protokol za razmjenu podataka
GCS	*(Ground Control Software)*	softver upravljačke zemaljske stanice
GCS	*(Ground Control System/Station)*	zemaljska upravljačka stanica

GDPR	*(General Data Protection Regulation)*	opća uredba o zaštiti podataka
GIS	*(Geographic Information System)*	geografski informacijski sustav
GLONASS	*(Globalnaya Navigatsionnaya Sputnikovaya Sistema)*	globalni navigacijski satelitski sustav - ruski
GNSS	*(Global Navigation Satellite System)*	globalni navigacijski satelitski sustav
GPS	*(Global Positioning System)*	globalni položajni sustav
ICCID	*(Integrated Circuit Card Identifier)*	identifikator mobilne mrežne kartice
IMEI	*(International Mobile Equipment Identity)*	međunarodni identifikator mobilne opreme
IMSI	*(International Mobile Subscriber Identity)*	međunarodni pretplatnički identifikator
IMU	*(Inertial Measurement Unit)*	inercijske mjerne jedinice
IP	*(Internet Protocol)*	mrežni protokol za prijenos podataka
JTAG	*(Joint Test Action Group)*	udruga elektroničkih industrija za razvijanje metode provjere dizajna i ispitivanja tiskanih pločica nakon izrade
LIDAR	*(Light Detection and Ranging)*	optički mjerni uređaj
LiPo	*(Lithium Polymer)*	litij-polimer (baterija)
MAC	*(Media Access Control)*	adresa za kontrolu pristupa medijima
MEID	*(Mobile Equipment Identifier)*	identifikator mobilne opreme
MSISDN	*(Mobile Station International Subscriber Directory Number)*	identifikator pretplate u globalnom sustavu za mobilne komunikacije
QR	*(Quick Response code)*	kod brzog odziva

RADAR	*(Radio Detection and Ranging)*	radio frekvencijski mjerni uređaj
RC	*(Radio Communication)*	radio komunikacija
RPAS	*(Remotely Piloted Aircraft System)*	daljinski upravljani zrakoplovni sustavi
RTH	*(Return To Home)*	navigacijski mehanizam povratka na početnu poziciju
SANS	*(Escal Institute of Advanced Technologies)*	privatna američka tvrtka specijalizirana za informacijsku sigurnost
SIM	*(Subscriber Identity Module)*	kartica za jednoznačno identificiranje korisnika na mreži
SMS	*(Short Message Service)*	usluga slanja kratkih tekstualnih poruka
SoC	*(System on a Chip)*	skup integriranih krugova za komponente mobilnog uređaja
SQL	*(Structured Query Language)*	strukturni upitni jezik
SSID	*(Service Set Identifier)*	identifikator postavljenog servisa
TAP	*(Test Access Ports)*	priključna mjesta na čipu
UAS	*(Unmanned Aerial System)*	bespilotni zrakoplovni sustavi
UAV	*(Unmanned Air Vehicles)*	bespilotni zrakoplovi
VTOL	*(Vertical Take Off and Landing)*	vertikalno uzlijetanje i slijetanje
WLAN	*(Wireless Local Area Network)*	bežična lokalna mreža

Popis slika

Slika 1. Izvedbe multikopter/multirotor bespilotnih zrakoplova 4
Slika 2. Dijelovi bespilotnog zrakoplova 8
Slika 3. Prikaz DJI Mavic Air bespilotnog zrakoplova 10
Slika 4. Prikaz unutarnje pohrane na kontroleru leta DJI bespilotnog zrakoplova 14
Slika 5. Zone protudjelovanja bespilotnim zrakoplovima 29
Slika 6. Primjeri C-UAS sustava 30
Slika 7. Princip ometanja lažiranjem GNSS koordinata 34
Slika 8. Primjer izvođenja i snimanja ručne ekstrakcije 41
Slika 9. Primjeri Chip-Off i JTAG tehnika 43
Slika 10. DJI Mavic Air uz daljinski upravljač te uređaj Sony Xperia Z1 46
Slika 11. Prikaz okruženja prilikom izvođenja letačkih operacija 46
Slika 12. Izvođenje ekstrakcije pomoću UFED Touch 2 alata 48
Slika 13. Prikaz *hash* vrijednosti za *dump* datoteku datotečne ekstrakcije 49
Slika 14. Primjer prikaza .SRT datoteke u jednoj slici videozapisa 50
Slika 15. Prikaz *debug_log* zapisa 51
Slika 16. Prikaz sučelja i mogućnosti DatCon programa 52
Slika 17. Prikaz podataka iz .CSV datoteke 52
Slika 18. Vizualni prikaz leta i *log* zapis unutar CsvView programa 53
Slika 19. Pregled osnovnih informacija o datotečnoj ekstrakciji 54
Slika 20. Primjer dohvaćenog tekstualnog, *log* podataka 55
Slika 21. Pregled osnovnih informacija o fizičkoj ekstrakciji 56
Slika 22. Dohvaćeni nekategorizirani i obrisani podaci 57
Slika 23. Prikaz dohvaćene lokacije videozapisa 58
Slika 24. Prikaz dohvaćenih fotografija i dodatnih podataka 58
Slika 25. Popis dohvaćenih metapodataka iz .EXIF datoteke 59
Slika 26. Prikaz baze podataka za letna ograničenja 60

Popis grafikona

Grafikon 1. Broj registriranih operatora bespilotnih zrakoplova u RH po godinama . 26

Grafikon 2. Učestalost korištenja bespilotnih zrakoplova u svijetu za 2017. po pojedinoj djelatnosti 27

Popis tablica

Tablica 1. Tehničke specifikacije DJI Mavic Air bespilotnog zrakoplova 10

Tablica 2. Kategorizacija bespilotnih letjelica u RH 1

Tablica 3. Korištena oprema prilikom provedbe forenzičke analize DJI Mavic Air-a. 45

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Forenzička analiza sustava bespilotnih zrakoplova**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 16.9.2020

Student/ica:

Klešćuš T.

(potpis)