Usporedni prikaz alata za postupak forenzičke analize sustava bespilotnih zrakoplova

Majić, Petar

Master's thesis / Diplomski rad

2021

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:119:761713

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Petar Majić

USPOREDNI PRIKAZ ALATA ZA POSTUPAK FORENZIČKE ANALIZE SUSTAVA BESPILOTNIH ZRAKOPLOVA

DIPLOMSKI RAD

Zagreb, veljača 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 2. studenoga 2020.

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

DIPLOMSKI ZADATAK br. 6058

Pristupnik: **Petar Majić (0135232891)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Usporedni prikaz alata za postupak forenzičke analize sustava bespilotnih zrakoplova**

Opis zadatka:

Prikazati karakteristike sustava bespilotnih zrakoplova kao terminalnih uređaja. Istražiti mogućnosti raznovrsnih alata digitalne forenzike. Razmotriti i opisati akvizicijsku metodologiju bespilotnih zrakoplova. Napraviti komparativnu analizu mogućnosti alata usmjerenih bespilotnim zrakoplovima. Istaknuti mehanizme digitalne antiforenzike i protumjere zloupotrebe bespilotnih zrakoplova.

Mentor:

dr. sc. Siniša Husnjak

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

USPOREDNI PRIKAZ ALATA ZA POSTUPAK FORENZIČKE ANALIZE SUSTAVA BESPILOTNIH ZRAKOPLOVA

COMPARATIVE PRESENTATION OF TOOLS FOR THE FORENSIC ANALYSIS PROCEDURE OF UNMANNED AERIAL SYSTEMS

Mentor: dr. sc. Siniša Husnjak

Student: Petar Majić

JMBAG:0135232891

Zagreb, veljača 2021.

ZAHVALA

Od srca zahvaljujem svome mentoru dr. sc. Siniši Husnjaku na uloženom trudu i vremenu te znanstvenim i stručnim savjetima kojima mi je puno pomogao u izradi ovoga diplomskoga rada.

Zahvaljujem i Fakultetu prometnih znanosti na ustupljenoj opremi i alatima korištenih pri izradi diplomskoga rada.

Posebice zahvaljujem svojoj djevojci te svim svojim prijateljima koji su mi pružili bezuvjetnu podršku tijekom studija i bez kojih moje studiranje ne bi bilo toliko zabavno i lako. Hvala vam na ohrabrenju i toplim riječima. Bez vas ništa ne bi bilo moguće jer mi niste dali da odustanem.

I na kraju, zahvaljujem svojoj obitelji koja je bila uz mene tijekom cijeloga školovanja te me svakodnevno hranila podrškom i ljubavlju. Hvala vam što ste mi pružili mogućnost da ostvarim svoje snove.

SAŽETAK

Ovaj diplomski rad prikazuje značajke forenzičke analize sustava bespilotnih zrakoplova. Razvojem bespilotnih zrakoplova, ali i povećanim korištenjem istih za nedozvoljene radnje, bespilotni zrakoplovi postaju interes digitalne forenzike. Osim bespilotnog zrakoplova, pod povećalom digitalne forenzike nalazi se kontroler za upravljanje kao i mobilni uređaj koji čine sustav bespilotnog zrakoplova. Kako postoji sličnost između bespilotnog zrakoplova i mobilnog uređaja, a metodologija još uvijek nije standardizirana, u ovome je radu zrakoplov analiziran metodologijom koja se koristi prilikom forenzičke analize mobilnog uređaja. Radom je dan pregled tijeka forenzičke analize sustava bespilotnog zrakoplova uz korištenje komercijalno dostupnih alata na tržištu. Odabir alata kao i metoda ekstrakcije podataka predstavljaju najveći problem prilikom istrage, stoga su usporedno prikazane mogućnosti forenzičkih alata s prednostima i nedostatcima. Detaljnom usporedbom takvih alata, lako je izvedivo procijeniti mogućnost pojedinog alata te utvrditi u kakvom je okruženju moguća upotreba. Osim alata, postoje metode antiforenzike poput skrivanja podataka ili manipulacija GPS prijemnika, koje su uspješne u prikrivanju dokaza. Protumjere letačkih aktivnosti predstavljaju još jedan izazov u borbi protiv zloupotrebe bespilotnih zrakoplova.

Ključne riječi**:** bespilotni zrakoplov; mobilni uređaj; digitalna forenzička analiza; ekstrakcija podataka; forenzički alat

SUMMARY

This master thesis presents the features of forensic analysis of drone systems. The development of drones and increased use of them for illicit activities lead to drones becoming the interest of digital forensics. Under the magnifying glass of digital forensics is a controller as well as a mobile device, together they make up the drone system. As there is a similarity between unmanned aerial vehicles and mobile devices, and the methodology hasn’t been standardized yet, in this research the aircraft is analyzed by the methodology used in forensic analysis of the mobile device. The paper provides an overview of the sequence of forensic analysis of unmanned aircraft systems using commercially available tools on the market. The choice of tools, as well as the method of data extraction, represents the biggest problem during the investigation. Therefore, the possibilities of forensic tools with advantages and disadvantages are presented. By comparing such tools, it is easy to assess the possibility of a particular tool and determine where it can be used. In addition to tools, there are anti-forensics methods such as hiding data or manipulating GPS receivers, which are successful in concealing evidence. Countermeasures against flying activities represent another challenge in the fight against the misuse of drones.

Keywords: UAV; mobile device; digital forensic analysis; data extraction; forensic tool

SADRŽAJ

1. Uvod 1
2. Karakteristike sustava bespilotnih zrakoplova kao terminalnih uređaja 2
2.1. Komponente bespilotnog zrakoplova 4
2.2. Karakteristike bespilotnog zrakoplova DJI Mavic Air 8
3. Prikaz mogućnosti raznovrsnih alata digitalne forenzike 11
3.1. Forenzički alati za mobilne uređaje 11
3.2. Alati za forenzičku analizu bespilotnih zrakoplova 14
4. Akvizicijska metodologija bespilotnih zrakoplova 19
4.1. Metodologija mobilne digitalne forenzike 20
4.2. Postupci i metode ekstrakcije podataka 23
4.2.1. Ručna ekstrakcija 24
4.2.2. Logička ekstrakcija 25
4.2.3. Hex dump 25
4.2.4. Chip-off 26
4.2.5. Micro read 27
4.2.6. Ekstrakcija podataka JTAG metodom 27
4.3. Izvori podataka sustava bespilotnog zrakoplova 28
5. Komparativna analiza mogućnosti alata usmjerenih bespilotnim zrakoplovima 32
5.1. Ekstrakcija podataka s DJI Mavic Air 35
5.2. Ekstrakcija podataka mobilnog uređaja 36
5.3. Analiza ekstrahiranih podataka 38
5.3.1. Analiza podataka ekstrahiranih alatom Cellebrite UFED Touch 2 38
5.3.2. Analiza podataka alatom Oxygen Forensics Detective 44
5.3.3. Analiza ručne ekstrakcije 49
5.4. Usporedba alata 53
6. Digitalna antiforenzika i protumjere zloupotrebe bespilotnih zrakoplova 56
6.1. Digitalna antiforenzika 56
6.1.1. Primjena digitalne antiforenzike na mobilni uređaj 56
6.1.2. Primjena digitalne antiforenzike na bespilotni zrakoplov 57
6.2. Protumjere zloupotrebe bespilotnog zrakoplova 58
6.2.1. Detektiranje bespilotnog zrakoplova 58
6.2.2. Zaustavljanje bespilotnog zrakoplova 59

7. Zaključak 61
Popis Literature 62
Popis slika 67
Popis tablica 68

1. Uvod

Digitalna forenzika je relativno mlada znanost koje se razvija posljednjih trideset godina. Zbog razvoja tehnologije i pojave novih uređaja digitalna forenzika sve više razvija smisao postojanja kao znanost. Posljednjih godina zabilježen je porast prodaje i upotrebe bespilotnih zrakoplova jer je njihovim razvojem omogućeno unaprjeđenje i olakšavanje provođenja raznih djelatnosti. Isto tako povećan je broj privatnih korisnika bespilotnih zrakoplova kao i kriminalnih i terorističkih organizacija koji su prepoznali mogućnost korištenja bespilotnih zrakoplova za ostvarivanje svojih ciljeva. Zbog navedenog, bespilotni zrakoplovi postaju predmet interesa forenzičkim istražiteljima diljem svijeta. Iako je forenzika bespilotnih zrakoplova još u svojim začecima, nema jasno definirane metodologije. Razvijeni su tek forenzički alati koji omogućavaju ekstrakciju i analizu podataka. Usporedba forenzičkih alata predstavlja primarni cilj ovoga rada i njihove mogućnosti bit će ispitane na sustavu bespilotnog zrakoplova kojega čine mobilni uređaj, kontroler i bespilotni zrakoplov DJI Mavic Air.

Rad se sastoji od sedam poglavlja:

1. Uvod
2. Karakteristike sustava bespilotnih zrakoplova kao terminalnih uređaja
3. Prikaz mogućnosti raznovrsnih alata digitalne forenzike
4. Akvizicijska metodologija bespilotnih zrakoplova
5. Komparativna analiza mogućnosti alata usmjerenih bespilotnim zrakoplovima
6. Digitalna antiforenzika i protumjere zloupotrebe bespilotnih zrakoplova
7. Zaključak

U drugome poglavlju ovoga rada, opisane su karakteristike sustava bespilotnog zrakoplova, komponente bespilotnog zrakoplova te karakteristike bespilotnog zrakoplova DJI Mavic Air. U trećem poglavlju prikazane su mogućnosti forenzičkih alata, na osnovu čega je lako uvidjeti prednosti i nedostatke.

U četvrtom poglavlju opisana je metodologija digitalne forenzike koja predstavlja nužne korake prilikom provođenja istrage, a prikazane su i metode ekstrakcije podataka koje je moguće primijeniti na bespilotni zrakoplov. Uz to, opisani su izvori dokaza sustava bespilotnog zrakoplova.

U petom poglavlju prikazane su, a zatim i uspoređene mogućnosti ekstrakcije te analize forenzičkih alata sustava bespilotnog zrakoplova. Na samome kraju tabličnim prikazom dan je uvid u mogućnosti korištenih alata kao i metoda ekstrakcije. A u posljednjem, šestom poglavlju opisane su metode antiforenzike, ali i protumjere kojima je moguće spriječiti zlonamjerne letačke aktivnosti.

2. Karakteristike sustava bespilotnih zrakoplova kao terminalnih uređaja

Sustav bespilotnih zrakoplova pod nazivom UAS (engl. *Unmanned Aerial System*) predstavlja jednu veliku suprotnost u odnosu na sve direktno upravljane letjelice. Budući da je riječ o bespilotnim letjelicama, njih prema službenoj literaturi nazivamo UAV (engl. *Unmanned Air Vehicles*). UAV pripada klasi zrakoplova koja može letjeti bez prisustva osobe (pilota) u samoj letjelici, što bi značilo da je ljudski faktor van same letjelice, najčešće na zemlji. Prema tome, u kategoriji UAV pripadaju razne inačice zrakoplova kojima se upravlja na daljinu, ali i one letjelice koje ne zahtijevaju upravljanje od strane čovjeka.

Danas, među najpoznatijim i najzastupljenijim komercijalnim bespilotnim letjelicama su tzv. dronovi, odnosno multikopteri. Kada je riječ o njima, svaki multikopter sastoji se od nekoliko elektromotora ovisno o izvedbi, te pomoću njih ostvaruje kretanje u zračnom prostoru (slika 1). Također, određene verzije UAV nemaju mogućnost samostalnog polijetanja i slijetanja pa se za potrebe polijetanja koriste lansirne rampe, a za slijetanje primjerice padobran.



Slika 1. Inačice multikopter bespilotnih zrakoplova
Izvor: [1], [2], [3]

Multikopteri prema svojim karakteristikama su više sličniji helikopterima nego zrakoplovima, čime su manje kompleksni, nemaju pokretne dijelove trupa niti krila, ali moraju imati nekoliko motora kako bi mogli izvoditi sve manevre u zračnom prostoru.

Zbog letnih sposobnosti, jednostavnosti rukovanja, brzina kretanja, mogućnosti vertikalnog slijetanja i polijetanja multikopteri su veoma poželjni u komercijalnoj, ali i u poslovnoj upotrebi. Dok su zrakoplovi prihvatljiviji, primjerice za vojne potrebe jer imaju mogućnost nositi veću količinu tereta te su, kao i multikopteri, upravljani na daljinu.

Kada je riječ o upravljanju bespilotnim letjelicama, ono može biti izvedeno na nekoliko načina. Najčešće se koriste posebno izrađeni kontroleri, ali je moguće letjeti i pomoću letačke aplikacije na mobilnom terminalnom uređaju. Osim navedena dva načina upravljanja, upotrebom kontrolera i mobilnog terminalnog uređaja, moguće je iskoristiti sve funkcionalnosti koje nudi zrakoplov.

Iako je uvriježeni naziv za bespilotne zrakoplove UAV, često ih se može pronaći pod nazivom RPAS (engl. *Remotely Piloted Aircraft System*). RPAS sustav također za potrebe upravljanja zahtijeva zemaljsku stanicu, gdje se komunikacija između letjelice i zemaljske stanice (kontrolera) odvija pomoću radio valova koje oboje odašilju i primaju, [4]. Ključne komunikacijske tehnologije koje se koriste za povezivanje, ali i upravljanje UAV su WiFi, GPS (engl. *Global Positioning System*) i drugi oblici radio komunikacije.

Podjela bespilotnih zrakoplova moguća je u više kategorija, ali ona osnovna je prema namjeni, odnosno vojni i civilni. Civilne bespilotne zrakoplove moguće je prema namjeni dodatno podijeliti na:

1. Rekreacijske bespilotne zrakoplove
2. Komercijalne bespilotne zrakoplove
3. DIY bespilotne zrakoplove

Rekreacijski bespilotni zrakoplovi su zrakoplovi koji prvenstveno nemaju sposobnost dugog leta, niske su cijene i ne nude funkcionalisti koje imaju komercijalni bespilotni zrakoplovi. Komercijalni bespilotni zrakoplovi imaju veću mogućnost primjene i iskorištavanja njihovih mogućnosti za komercijalne potrebe. Treća vrsta bespilotnih zrakoplova su tzv. DIY (engl. *Do It Yourself*), odnosno „Uradi sam“ zrakoplovi. Ovakvi zrakoplovi se izrađuju prema želji korisnika i omogućavaju razne modifikacije i stalne izmjene na zrakoplovu koje nije moguće izvesti na prethodna dva tipa.

Klasifikacija civilnih bespilotnih zrakoplova na razini EU regulirana je od strane EASA (engl. *European Union Aviation Safety Agency*). EASA je Europska agencija za zrakoplovnu sigurnost te je zadužena za certifikaciju, regulaciju i standardizaciju kao i istrage i nadzor zrakoplovstva.

Tablica 1. prikazuje klasifikaciju bespilotnih zrakoplova bez oznake klase na području EU koja je važeća do 1. siječnja 2023. Nakon navedenog datuma stupa izmjena i vrijedit će nova pravila prema kojima će svi bespilotni zrakoplovi morati biti klasificirani.

Tablica 1. Ograničenja za bespilotne zrakoplove bez oznake klase

<table>
<tr><th colspan="2">UAS</th><th colspan="2">Operacije</th><th colspan="3">Operator/pilot</th></tr>
<tr><th>Klasa</th><th>MTOM</th><th>Potkategorija</th><th>Ograničenja</th><th>Registracija</th><th>Edukacija operatora</th><th>Minimalna dobna granica</th></tr>
<tr><td>Privatno izrađeni</td><td>< 250 g</td><td rowspan="2">A1 (može letjeti u potkategoriji A3)</td><td rowspan="2">Zabrana leta iznad ljudi</td><td>Ne (osim ako posjeduje kameru)</td><td>Nije potreban trening</td><td>Ne</td></tr>
<tr><td>Bez oznake klase</td><td>< 500 g</td><td>Da</td><td rowspan="3">Pročitati korisnička uputstva, završiti trening i položiti ispit</td><td>16</td></tr>
<tr><td>Bez oznake klase</td><td>< 2 kg</td><td>A2 (može letjeti u potkategoriji A3)</td><td>Zabrana leta iznad ljudi, horizontalna udaljenost 50m od ljudi</td><td>Da</td><td>16</td></tr>
<tr><td>Bez oznake klase ili privatno izrađeni</td><td>< 25 kg</td><td>A3</td><td>Zabrana leta iznad ljudi, 150m udaljenosti</td><td>Da</td><td>16</td></tr>
</table>

Izvor: [5]

2.1. Komponente bespilotnog zrakoplova

Bespilotni zrakoplovi, kao i zrakoplovi općenito, dijele mnoge fizičke komponente. Ključna je razlika u kokpitu, odnosnu upravljačkom sustavu. Komponente bespilotnih letjelica poput raznih senzora (npr. kamera) ili nosača tereta nisu nužne za letačke aktivnosti, ali proširuju mogućnosti korištenja samog zrakoplova. Kako bi mogao letjeti i izvršavati radnje, bespilotnom zrakoplovu potrebne su sljedeće opisane komponente.

Okvir predstavlja glavni element svakog bespilotnog zrakoplova, koji je najčešće izrađen od plastičnih polimera, ugljičnih vlakana ili aluminija. Ovisno o izvedbi same bespilotne letjelice, okvir štiti komponente od oštećenja.

Propulzija svakog zrakoplova čine motor ili više njih, propeleri, baterije i ESC (engl. *Electronic Speed Controller*). Bez obzira radi li se o VTOL, multikopter izvedni svakoj letjelici su potrebne navedene komponente za mogućnost leta. Motor i propeleri omogućavaju operacije letenja, uzlijetanja i slijetanja pomoću energije koja je uskladištena u Li-Po baterijama. Određene inačice UAV umjesto elektromotora koriste konvencionalne zrakoplovne motore. Za UAV koji koriste elektromotore nužno je imati i ESC.

Elektronički kontroleri brzine (ESC) uređaji su koji omogućavaju kontrolerima leta dronova kontrolu i prilagodbu brzinu elektromotora zrakoplova. Signal kontrolera leta uzrokuje da ESC po potrebi poveća ili smanji napon na motoru, mijenjajući tako brzinu propelera. Elektroničke kontrole brzine mogu se nositi i s aktivnim ili regenerativnim kočenjem, postupkom kojim se mehanička energija motora pretvara u električnu energiju koja se može koristiti za punjenje baterije bespilotnog zrakoplova. Tijekom razdoblja u kojima se dron usporava, motor može djelovati kao generator, a ESC obrađuje višak struje koji se može vratiti u bateriju, [6].

Kako bi se sačuvali elementi propulzije letjelice, izrađeni su posebni štitnici koji štite od bilo kakvih oštećenja u slučaju kolizije. Osim što štite od oštećenja, sami štitnici mogu spriječiti kontakt propelera s preprekama i tako spriječiti pad same letjelice i veće materijalne gubitke. Štitnici za letjelice još uvijek nisu standardni te ih određeni proizvođači nude uz nadoplatu, dok za neke modele ne postoji nikakav oblik zaštite kako motora, tako ni propelera.

Bespilotne letjelice zahtijevaju softverske i hardverske elemente za kontrolu leta koji će omogućiti daljinsko upravljanje zrakoplovom, bilo izravno od pilota ili autonomno od računala, a za to je potreban kontroler leta. Dinamika leta UAV-a vrlo je promjenjiva i nelinearna, pa će održavanje položaja i stabilnosti možda zahtijevati kontinuirano računanje i prilagodbu letačkih sustava. Elementi kontrolera leta na tlu čine dio GCS (engl. *Ground Control Station*) i uključuju modem i podatkovnu vezu za komunikaciju s UAV-om, kontroler za ručnu kontrolu zrakoplova i GCS softver. Elementi u zrakoplovu uključuju autopilot, vezu za komunikaciju s GCS-om i periferne uređaje kao što su vanjski magnetometri i GNSS (engl. *Global Navigation Satalite System*) prijamnici, [7].

GNSS prijemnik je modul koji omogućuje komunikaciju bespilotne letjelice sa satelitskim sustavima za potrebe pozicioniranja same letjelice i određivanje visine letjelice. Letjelice koje posjeduju GNSS prijemnik imaju mogućnost automatskog vraćanja na lokaciju s koje je letjelica poletjela, što je izuzetno korisno ako letjelica izgubi kontakt s kontrolerom.



Slika 2. Komponente UAS, [8]

Radio prijemnik čine antenski sustav i elektronički modul na letjelici namijenjen prijemu upravljačkih signala za letjelicu koji se odašilju s radio odašiljača. Radio odašiljač sastoji se, kao i prijemnik, od antenskog sustava i elektroničkog modula pomoću kojega operator upravlja zrakoplovom, odnosno šalje upravljačke signale letjelici. Radio odašiljač predstavlja kontroler, odnosno daljinski upravljač u slučaju manjih letjelica ili kontrolnu postaju koju koristi vojska za veće letjelice.

Senzore čine elektronički moduli ili zasebni uređaji koju omogućavaju primjenu UAV za razne svrhe. UAV koriste širok raspon instrumenata i senzora za poboljšanje rada ili za prikupljanje podataka. Povezani trend je integracija više UAV instrumenata kako bi se poboljšala funkcionalnost što je više moguće u jednom sustavu, [9].

Senzori koje koriste bespilotni zrakoplovi su:

- Akcelerometar – osjetljivi senzor koji na osnovi količinu sile ubrzanja manevra može odrediti poziciju letjelice.
- Magnetometar – elektronički kompasi daju informacije o smjeru inicijalnih sustava za navigaciju i vođenje. AMR senzori imaju vrhunske karakteristike točnosti i vremena odziva, a troše znatno manje energije od alternativnih tehnologija, vrlo su pogodni za primjenu u bespilotnim letjelicama.
- Senzori inercije – mjerenje inercije u kombinaciji s GPS-om ključno je za održavanje smjera i putanje leta. Kako bespilotni zrakoplovi postaju autonomniji, oni su ključni za održavanje poštivanja pravila leta i kontrole zračnoga prometa.

- Senzor nagiba – u kombinaciji sa žiroskopima i akcelerometrima, daju ulaz u sustav kontrole leta kako bi se održao nivo leta. To je izuzetno važno za primjene u kojima je stabilnost najvažnija, od nadzora do isporuke krhke robe. Ove vrste senzora kombiniraju akcelerometre sa žiroskopima, što omogućuje otkrivanje malih varijacija kretanja, [10].
- Senzori struje – u bespilotnim zrakoplovima važna je potrošnja i upotreba energije. Senzori struje mogu se koristiti za nadgledanje i optimizaciju odvoda energije, sigurno punjenje unutarnjih baterija i otkrivanje stanja kvarova na motorima ili drugim dijelovima sustava. Senzori s brzim vremenom odziva i velikom preciznošću optimiziraju vijek trajanja baterije i performanse bespilotnog zrakoplova.
- LiDAR - vrsta senzora koja za potrebe tehnologije udaljenog otkrivanja koristi brze laserske impulse za mapiranje površine zemlje. LiDAR je koristan kada se koristi za stvaranje prikaza digitalnih površina, modela terena i visina, [11].

Osim već navedenih senzora koriste se i ovi senzori: kamera, GPS senzori, termalni senzori i ostalo.

Zrakoplovi osim komponenti (hardvera) zahtijevaju i operativni sustav (softver) kako bi mogli obavljati letačke aktivnosti, ali i određene dodatne radnje (npr. snimanje kamerom, mjerenje udaljenosti i sl.). I sam kontroler, odnosno upravljačka zemaljska stanica, zahtijeva operativni sustav.

Komercijalne letjelice koje se nalaze na tržištu već posjeduju ugrađeni softver i operater letjelice ima mogućnost nadogradnje toga softvera od strane proizvođača. Za razliku od komercijalnih letjelica, DIY letjelice koje su sastavljane od različitih komponenti, omogućavaju korištenje različitih softverskih rješenja, najčešće je to open source softver.

FMS (engl. *Flight Management Software*) je softver za upravljanje letom bespilotnih letjelica i letjelica koje zahtijevaju prisustvo posade u samoj letjelici. Osim namjene upravljanja prilikom uzlijetanja i slijetanja, FMS omogućava dodatne funkcionalnosti kao unos navigacijskih parametara. Također, FMS je ključan u primjeni bespilotnih zrakoplova jer on omogućava komunikaciju između komponenti zrakoplova i kontrolera.

GCS (engl. *Ground Control Software*) je softver čija je namjena upravljanje predodređenim navigacijskim rutama ili operacijama. Najčešće se sastoji od baze podataka zona letenja te mehanizama za obradu podataka dobivenih iz senzora. GCS se primjenjuje na samim stanicama za upravljanje.

2.2. Karakteristike bespilotnog zrakoplova DJI Mavic Air

Za potrebe praktičnoga dijela ovoga diplomskoga rada, odnosno provođenja forenzičkog istraživanja i analize, korištena je bespilotna letjelica DJI Mavic Air (slika 3). DJI Mavic Air je bespilotni zrakoplov kojega pokreću četiri motora, a svjetlo dana ugledao je 2018. godine. Riječ je o sklopivom zrakoplovu koji ima relativno male dimenzije, ali unatoč tome nudi iznimne performanse i pruža pregršt mogućnosti. Tada je to bio najmanji komercijalni bespilotni zrakoplov koje je posjedovao stabilizator u tri osi, ali i odličan sustav za izbjegavanje prepreka u tri smjera.



Slika 3. Bespilotni zrakoplov DJI Mavic Air i kontroler, [12]

Za potrebe upravljanja letjelicom DJI Mavic Air potreban je kontroler ili pametni mobilni uređaj uz prethodno instaliranu DJI GO 4 letačku aplikaciju. Za bolje iskustvo i sigurniji let moguće je koristi kontroler i pametni terminalni uređaj, gdje se kontroler koristi za upravljanje letjelicom, a mobilni uređaj za prijenos slike u stvarnom vremenu te postavljanje postavki sustava zrakoplova.

Ako za let koristi samo pametni mobilni uređaj, domet letjelice je puno manji, a korištenjem kontrolera bez pametnog mobilnog uređaja gube se razne funkcionalnosti (npr. Smart Capture, ActiveTrack). Mavic Air koristi „Enhanced WiFi“ za potrebe komunikacije s kontrolerom, gdje se u podvozju zrakoplova nalazi omnidirekcionalna antena, [13].

Tablica 2. Tehničke specifikacije DJI Mavic Air bespilotnog zrakoplova

Bespilotni zrakoplov	
Najveća masa uzlijetanja	430 g
Dimenzije sklopljene letjelice	168x83x39 mm (DxŠxV)
Dimenzija raskloplјene letjelice	168x184x64 mm (DxŠxV)
Maksimalna brzina uzlijetanja (vertikalno)	4 m/s (S mod) 2 m/s (P mod)
Maksimalna brzina slijetanja (vertikalno)	3 m/s (S mod) 1.5 m/s (P mod)
Maksimalna brzina leta	68.4 km/h (S mod)m 28.8 km/h (P mod)
Maksimalno vrijeme leta (bez vjetra)	21 min pri brzini od 25km/h
Maksimalna udaljenost pri letu (doseg)	10 km
Maksimalna otpornost na brzinu vjetra	29-38 km/h
GNSS	GPS + GLONASS
Unutarnja pohrana	8 GB
Podrška SD kartice	microSD (Class 10 ili UHS -1)
Baterija	
Kapacitet	2375 Mah
Napon	11.55 V
Tip	LiPo 3S
Sustav snezora	
Domet mjerenja	0.5-12 m naprijed, 0.5-10 m straga
Domet detekcije	0.5-24 m naprijed, 0.5-20 m straga
Efektivna brzina pri osjetu	≤8 m/s
Gimbal	
Stabilizacija	3 osi (nagib, rotacija, pomicanje)
Maksimalna brzina kontrole	120 °/s
Raspon kutnih vibracija	±0.005°
Kamera	
Senzor	1/2.3” CMOS, 12 MP
Leća	FOV: 85°, 35 mm f/2.8
Rezolucija fotografija	4:3: 4056×3040, 6:9: 4056×2280

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
Podržani format datotečnog sustava	FAT32
Podržani format fotografija / video zapisa	JPEG/DNG (RAW) / MP4/MOV (H.264/MPEG-4 AVC）
Kontroler	
Radna frekvencija	F1 : 2.400 - 2.4835 GHz F2 : 5.725 - 5.850 GHz
Maksimalna udaljenost odašiljanja (bez interferencije)	F1 : 2000 – 4000 m F2 : 500 – 4000 m
Snaga odašiljanja	F1 : ≤26 F2 : ≤30
Podržane dimenzija mobilnih uređaja	Maksimalna dužina : 160 mm Podržana debljina 6.5 – 8.5 mm
Podržani USB priključci kontrolera	Lightning, MicroUSB (TYpe-B), USB-C
Baterija	2970 mAh
Aplikacija DJI GO 4	
Sustav prijenosa videa	Enhanced WiFi
Kvaliteta videa uživo	720p/30fps
Latencija	170 – 240 ms
Operativni sustav	Android, iOS

Izvor: [14]

Prema karakteristikama prikazanim tablicom 2, vidljivo je kako relativno mali bespilotni zrakoplov DJI Mavic Air posjeduje i neke od karakteristika većih bespilotnih zrakoplova. Autonomija baterije u praksi je nešto manja nego što je deklarirana ali letačke sposobnosti zrakoplova su iznimnome dobre, te je vrlo lako savladati kontrole ovog bespilotnog zrakoplova.

3. Prikaz mogućnosti raznovrsnih alata digitalne forenzike

Forenzička analiza sustava bespilotnih letjelica slična je analizi računala i mobilnog uređaja, ali postoje određene razlike. Neke od najvažnijih razlika su količina potencijalnih dokaza te raznolikost hardvera i softvera. Bitno je spomenuti razliku u osjetljivosti podataka koja je prisutna i kod mobilnih uređaja koji su dio toga sustava. Naravno, prisutan je i problem nemogućnosti izvođenja ekstrakcije i analize DIY letjelica u odnosu na ionako maleni broj podržanih komercijalnih letjelica.

Forenzički alati koji su dostupni na tržištu za oporavak dokaza sastoje se od hardvera koji obuhvaća razne kablove za povezivanje letjelice, mobilnog uređaja i radne stanice ili uređaja za ekstrakciju. Softver je potreban kako bi se izdvojili potrebni dokazi, provela analiza i kreirao izvještaj.

3.1. Forenzički alati za mobilne uređaje

Kako je mobilni uređaj dio sustava bespilotne letjelice, on je često neophodan u samoj forenzičkoj istrazi. Ovisno o samom modelu uređaja, kao i korištenom alatu, moguće je doći do bitne količine dokaza koju je kasnije moguće iskoristiti u sudskom procesu. Često prilikom provođenja istrage sam mobilni uređaj može sadržavati bitne dokaze dok bespilotna letjelica nema tu mogućnost.

Prilikom provođenja forenzičke analize, poželjno je koristiti što više alata kako bi sama ekstrakcija podataka i analiza dale što više dokaza. Kada je riječ o samim forenzičkim alatima za mobilne uređaje, neki od njih podržavaju i izvođenje forenzičke akvizicije nad bespilotnim zrakoplovima poput UFED Physical Analyzer i Oxygen Forenscis Detective.

Danas je dostupno mnogo alata od kojih su jedni komercijalne prirode (UFED, Oxygen Detective, MSAB XRY), a drugi otvorenog koda (Autopsy i iPhone Analyzer). Mogućnosti nekih od alata navedeni su u tablici ispod.

Tablica 3. Mogućnosti forenzičkih alata za forenzičku analizu mobilnih uređaja

KARAKTERISTIKE	FORENZIČKI ALATI				
	XRY Logical	Paraben DDS	MOBILedit!	Oxygen Forensics Detective	Cellebrite Physical Analyzer
Metode prikupljanja podataka					
Logičke datoteke	DA	DA	DA	DA	DA
Memorijska kartica	DA	DA	NE	DA	DA
Fizički izvadak[1]	DA	DA	DA	DA	DA
Analiza podataka					
Označavanje	NE	DA	NE	DA	DA
Hex preglednik	NE	DA	DA	DA	DA
Tekstualni preglednik	NE	DA	DA	DA	DA
Multimedijske datoteke	NE	DA	NE	DA	DA
Usporedba podataka	DA	DA	NE	DA	DA
Oporavak podataka	DA	DA	DA	DA	DA
Sortiranje podataka	NE	DA	NE	DA	DA
Mogućnost mapiranja	DA	NE	NE	NE	NE
Preglednik slika	NE	DA	DA	DA	DA
Preglednik registra[2]	NE	DA	NE	DA	NE
Potvrda integriteta podataka					
MD-5	NE	DA	DA	DA	DA
SHA-1	NE	DA	NE	DA	DA
SHA-256	NE	NE	NE	DA	DA
Podrška SIM kartica					
GSM	DA	DA	DA	DA	DA
CDMA	NE	NE	NE	DA	NE
Kloniranje SIM kartice	DA	DA	DA	NE	DA
USIM	DA	DA	NE	NE	DA
Formati izvještaja					
CSV	NE	NE	NE	DA	DA
HMTL	NE	NE	DA	DA	DA
PDF	NE	NE	NE	DA	DA
TXT	NE	NE	DA	NE	NE
XML	DA	NE	DA	DA	DA

Izvor: [15]

[1] Fizički izvadak sadržaja iz uređaja
[2] Preglednik registra Windows CE

Cellebrite je izraelska tvrtka specijalizirana za izradu alata za potrebe ekstrakcije i analize podataka raznih uređaja. UFED Touch 2 je najpoznatiji produkt tvrtke Cellebrite te predstavlja izuzetno snažan alat za fizičku i logičku ekstrakciju raznih uređaja (uključujući GPS uređaje, bespilotne letjelice). Physical Analyzer je softverski alat namijenjen čitanju UFED datoteke (UFED dump datoteke formata.ufd) i UFED izvješća (.xml), [16].

UFED se sastoji od dvije komponente, [16]:

- UFED Touch 2 (slika 4) s dodatnim modulima koji se koriste za provođenje ekstrakcije podataka s raznih uređaja ili SIM (engl. *Subscriber Identity Module*) kartica, a koje se zatim mogu spremiti na USB disk, SD memorijsku karticu ili izravno na računalo.

- UFED Physical Analyzer, softver koji omogućuje izvođenje analize podataka nastalih kao dio ekstrakcije te stvaranje izvještaja.



Slika 4. Forenzički alat Cellebrite UFED Touch 2, [17]

Paraben DDS (engl. *Deployable Device Seizure*) mnogi stručnjaci smatraju kao jednim od najboljih i najbržih alata za dohvaćanje podataka s mobilnog uređaja. Sukladno tome ovaj alat je često prvi izbor za ekstrakciju podataka mobilnog uređaja ali i drugih uređaja.

Ovaj alat dostupan je na tablet uređajima koji se koriste na licu mjesta događaja tijekom ispitivanja mobilnog uređaja, raznih drugih uređaja i SIM kartica. Cilj ovog alata je pomoći forenzičkim stručnjacima u brzom pronalasku dokaza. Paraben DDS omogućava dohvaćanje podataka velikog broja mobilnih uređaja, približno 4000, kao i otključavanje istih, [18].

Oxygen Forensics Detective je forenzički softver za fizičku i logičku analizu mobitela, pametnih telefona, bespilotnih zrakoplova i memorijske kartice razvijen od strane tvrtke Oxygen Forensics. Omogućava izdvajanje informacija o uređaju, kontakte, SMS (engl. *Short Message Service*) poruke, razne datoteke, podatke o aplikacijama i ostalo. Ovaj alat omogućava izdvajanje metapodataka[3] iz uređaja, poput lokacije fotografiranja određene fotografije što je izuzetno korisno prilikom analize uređaja te očitavanje informacija o mrežnim aktivnostima, [19].

MOBILedit Forensics jedini je alat od navedenih koji omogućava bežično povezivanje mobilnog uređaja putem Wi-Fi. Podržava većinu uređaja koji su trenutno dostupni na tržištu, kao i veliki broj generičkih uređaja kineskih proizvođača, [20].

XRY Logical je samo jedan od alata tvrtke MSAB. Ovaj alat koristi se za analizu, ali i oporavak izbrisanih podataka s mobilnih uređaja, GPS uređaja i tableta. Kako bi ekstrahirao podatke s digitalnih uređaja, ovaj alat komunicira s operativnim sustavom uređaja. Cijeli proces ekstrakcije je automatiziran, a ovakva ekstrakcija je ekvivalent ručnog pregledavanja uređaja i snimanju onoga što se nalazi na njemu, [21].

3.2. Alati za forenzičku analizu bespilotnih zrakoplova

Bespilotni zrakoplovi kao i mobilni uređaji mogu sadržavati važne dokaze. Tijekom pronalaženja podataka, pa čak i onih skrivenih ili izmijenjenih, koriste se kao i kod forenzike mobilnih uređaja razni forenzički alati.

Kao i za alate u prethodnom poglavlju, glavna svrha alata je pružanje pomoći istražiteljima u istrazi, ali uz to oni rade i na ubrzanju tijeka istrage. Umjesto ručnog pretraživanja svih dokaza i analize, cijeli proces je automatiziran, a istražitelj ima mogućnost filtriranja i odabira načina pretrage i sl.

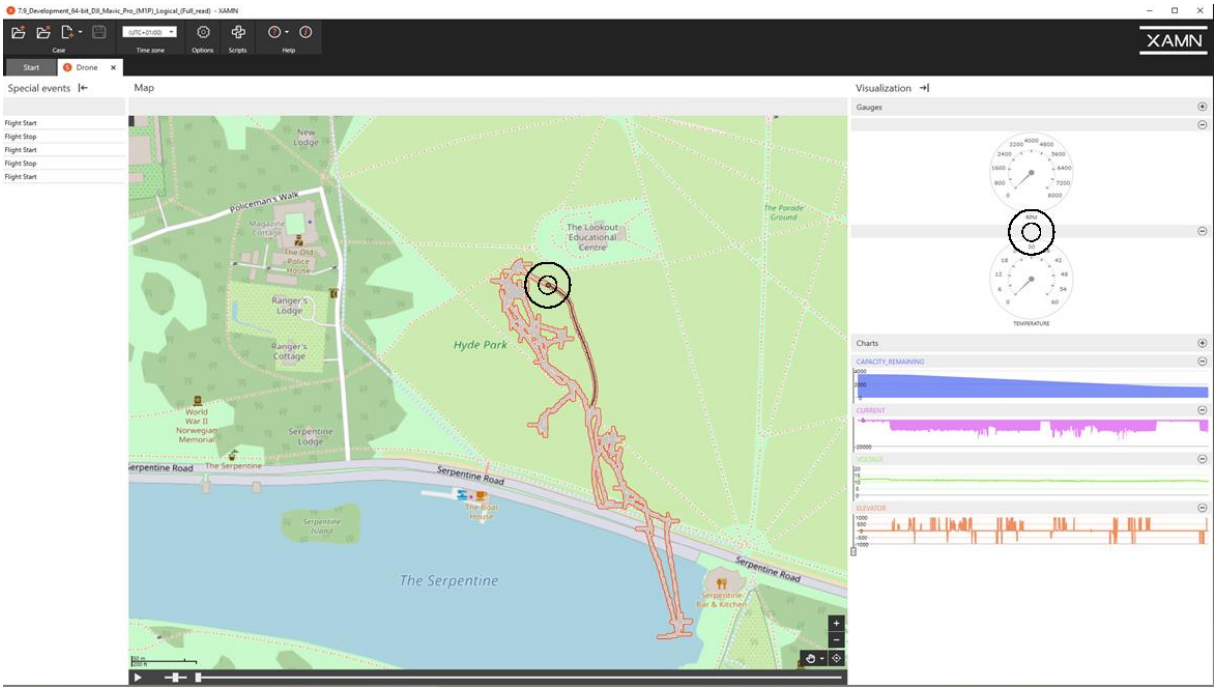
Budući da je forenzika bespilotnih zrakoplova među posljednje razvijenim granama digitalne forenzike, još uvijek na tržištu ne postoji veliki broj alata za ekstrakciju i analizu podataka s letjelica. Alati koji su korišteni za potrebe praktičnog dijela rada, u 5. poglavlju bit će detaljnije opisani. Samim time bit će vidljive razlike između njih, počevši od same podrške modela letjelica, do mogućnosti ekstrakcije, analize i u konačnici, stvaranja izvještaja.

[3] Metapodatci su podatci koji opisuju karakteristike digitalnih podataka.

Dostupni alati za provođenje forenzičke analize i ekstrakcije podataka bespilotnih letjelica su Cellebrite UFED Touch 2, Cellebrite Physical Analyzer, Oxygen Forensics Detective, XRY Drone, Acces Data FTK Imager i Quin-C i drugi.

Razne agencije širom svijeta razvijaju posebne metode za smanjenje prijetnji bespilotnih letjelica. Kada je bespilotna letjelica uključena u kazneno djelo, istražitelji će posegnuti za nekim od alata kako bi mogli izvršiti ekstrakciju podataka, analizirali ih i dokaze predstavili sudu ili nekom od nadležnih tijela na njima razumljiv način. XRY Drone samo je jedan od alata koji je moguće koristiti.

XRY Drone omogućuje korisnicima ekstrakciju i analizu podataka pronađenih u najpopularnijim komercijalnim zrakoplovima tvrtke DJI. MSAB aktivno radi na istraživanju područja forenzike bespilotnih zrakoplova i dodaje podršku za nove modele dronova i aplikacija. Zbog vlastitog vlasničkog formata datoteke, ovaj alat osigurava integritet lanca dokaza, što je presudan čimbenik prilikom svake istrage. XRY Drone dodatak je na postojeće alate za ekstrakciju tvrtke MSAB.

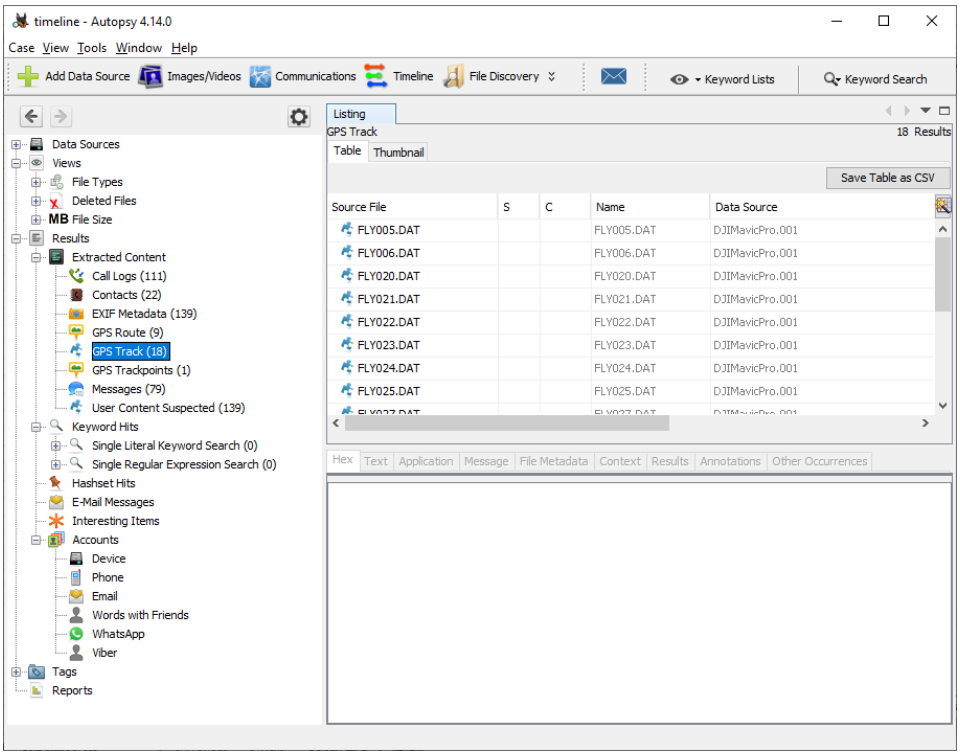


Slika 5. Sučelje alata XRY Drone, [22]

Ekstrahirani podatci iz letjelice mogu biti pregledani, analizirani te je, naposljetku, moguće kreirati izvještaj pomoću XMAN Viewer. Videozapisi i slike nastali korištenjem bespilotnog zrakoplova gledaju se na isti način kao multimedijski sadržaj s mobilnih telefona, dok podaci o putu leta mogu biti vizualizirani u specijalnoj kartici XAMN Drone. Kartica Drone koristi interaktivnu kartu koja pokazuje kada, gdje i kako je upravljano bespilotnim zrakoplovom. Skup mjerača i karata može prikazati informacije o potrošnji energije, položaju, nadmorskoj visini, brzini, rotiranju i nagibu drona.

Primjerice, iznenadni pomak u potrošnji energije može točno ukazati kada i gdje korisni teret je ispušten. Kombinacijom XRY Drone s XAMN-om moguće je ostvariti oporavak, dekodiranje i prikaz vrijednih podataka o letu iz bespilotnog zrakoplova pod istragom, [23].

U svijetu digitalne forenzike našao se i Autopsy, alat otvorenog koda, što znači da je potpuno besplatan, ali edukacija i licenciranje se naplaćuje od strane tvrtke Basis Technology. Ovaj je alat izrazito jednostavan za korištenje, grafičko sučelje je dizajnirano intuitivno. Zbog mogućnosti rada na nekoliko paralelnih zadataka, moguće je brzo doći do željenih rezultata.



Slika 6. Autopsy GPS Track, [24]

Autopsy podržava analizu podataka bespilotnih zrakoplova, ali za sada je to samo mali broj podržanih letjelica. Omogućava analizu *imagea* koji je prethodno ekstrahiran sa SD kartice DJI letjelica (Mavic Air & Pro, Inspire 1 & 2, Phantom 3, 4 & 4 Pro). Prilikom provođenja analize bespilotne letjelice moguće je pratiti GPS koordinate nastalih medijskih datoteka, kao i rutu leta.

Mogućnosti alata, [25]:

- Analiza vremenske trake događaja - napredno grafičko sučelje za pregled događaja (video zapis uključen)
- *Hash* filtriranje
- Traženje ključnih riječi - indeksirano pretraživanje ključnih riječi za pronalaženje datoteka koje spominju relevantne pojmove
- Web artefakti - izdvajanje povijesti, oznaka i kolačića iz Firefoxa, Chromea i IE
- *Data carving* - oporavak izbrisanih datoteka iz neraspoređenog prostora pomoću PhotoRec-a
- Multimedija - izdvajanje EXIF iz slika i videozapisa

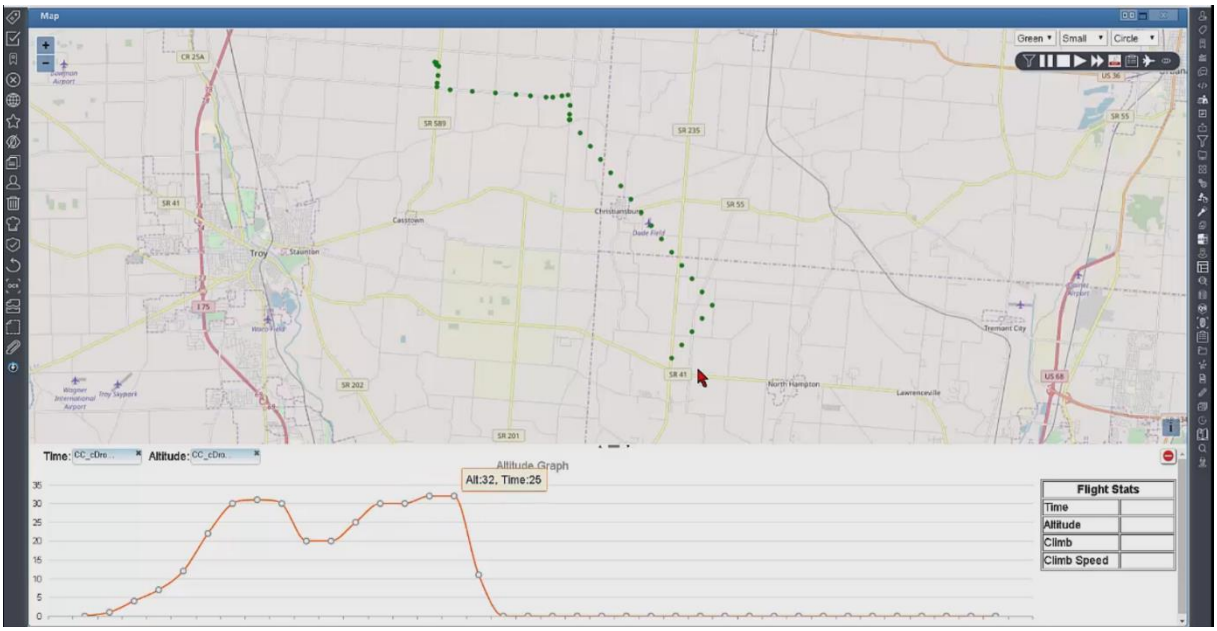
Tvrtka Access Data je, kao i ostali konkurenti, prisutna u forenzici dronova, ali ipak ne na toj razini kao konkurencija. Jedan od alata kojeg je moguće koristiti za ekstrakciju podataka je FTK Imager. Ovaj alat može kreirati *image* bilo kojeg sustava ili tipa memorije bez ikakvog utjecaja na integritet dokaza. FTK Imager može biti korišten za verifikaciju *hash* funkcije *image*-a, pregled datoteka i *image*, oporavak izbrisanih datoteka te izvoz datoteka iz *image*-a, [26].

FTK Imager nema mogućnost pregleda tijeka događaja kao ni mogućnost pregleda, odnosno pronalaska koordinata lokacije fotografije ili video zapisa zabilježenih letjelicom. Za te je potrebe moguće koristiti softver DatCon u kombinaciji s FTK Quin-C za potrebe analize i vizualizacije.

DatCon je softver koja čita .DAT datoteku, a zatim stvara izlazne datoteke koje sadrže izvučene podatke. Te izlazne datoteke je tada moguće očitati pomoću Excel-a, ali i pomoću Quin-C. Quin-C je poželjno koristiti jer omogućava bolji uvid u vrijeme gdje je letjelica letjela na temelju GPS podataka kao i visinu letjelice (slika 7).

DatCon podržava rad s .DAT datotekama sa DJI letjelica: Phantoma 3, Inspire 1, Mavic, Mavic Air, Mavic Pro i Phantom 4, Phantom 4 Pro, Inspire 2, Matrice M100, M600 kao i .DAT datoteke koji su kreirale aplikacije Go and Fly za sve platforme, osim za Mavic Mini 2, [27].

Praćenje mrežnog prometa između pametnog mobilnog uređaja i bespilotnog zrakoplova pripada domeni mrežne forenzike. Neki od alata koju se mogu koristiti su Nmap, Wireshark i Xplico. Presretanjem prometa pomoću Nmap-a, vrši se skeniranje portova, pronalaze se IP i MAC adrese, a isto tako moguće je i otkriti koji su portovi otvoreni. Korištenjem Wiresharka moguće je prikupiti pakete u bežičnoj komunikaciji između letjelice i mobilnog uređaja/kontrolera.



Slika 7. Prikaz letačkih aktivnosti bespilotne letjelice alatom FTK Quin-C, [28]

Sav prometa koji nastaje je kriptiran i većina prometa je forenzičkim stručnjacima nedostupna i beskorisna, ali određeni podatci poput stvarnih vremenskih podataka telemetrije mogu biti korisni dokazi u slučaju, [29].

4. Akvizicijska metodologija bespilotnih zrakoplova

U prethodnim poglavljima prikazano je kako je digitalna forenzika bespilotnih zrakoplova slična forenzici računala, ali i forenzici mobilnih uređaja. No, prema načinu pristupa samom slučaju, načinu povezivanja uređaja i drugih sličnosti, forenziku bespilotnih zrakoplova možemo poistovjetiti s forenzikom pametnih mobilnih uređaja.

Pristup samom procesu slučaju je izuzetno bitan, uz to bitno je poštivati lanac posjeda dokaza kako bi očuvali pronađene dokaze i kako bi isti bili prihvaćeni na sudu. Također, bitan je i odabir metodologije.

Digitalni istražitelji često obavljaju sve potrebne zadatke; od prikupljanja, dokumentiranja, čuvanja digitalnih dokaza do izdvajanja korisnih podataka kako bi se kreirala jasnija slika istrage kao cjeline. Istražiteljima je potrebna metodologija koja im pomaže obavljati sve zadatke ispravno, a kako bi oni došli do znanstvene istine koje će iskoristiti kao dokaze na sudu.

Pravosuđe je jedno od područja gdje je forenzička znanost korisna, nudeći pažljivo provjerene metode za obradu i analizu dokaza te dolaženje do zaključka koji se može reproducirati.

Cilj forenzičke analize prvobitno je pronaći počinjena dijela bespilotnim zrakoplovom te povezati zrakoplov s aplikacijom, odnosno kontrolerom za upravljanje koji bi trebao dovesti do korisnika, odnosno vlasnika istog tog zrakoplova. Forenzika sustava bespilotnih zrakoplova objedinjuje nekoliko grana forenzike za potrebe prikupljanja, ispitivanja i analize podataka kao što je vidljivo iz tablice 4.

Tablica 4. Primjena raznolikih grana forenzike u području forenzike bespilotnih zrakoplova

Komponente	Grana forenzike
Upravljačka aplikacija	Forenzika mobilnih uređaja
Bespilotni zrakoplov	Računalna forenzika-Linux
Kontroler	Mrežna forenzika
Pohrana	Standardne metode digitalne pohrane
Cloud pohrana	Cloud forenzika

Izvor: [30]

4.1. Metodologija mobilne digitalne forenzike

U svijetu digitalne forenzike prisutno je nekoliko različitih metodologija digitalne forenzike, neke od njih nisu toliko detaljne i nisu dobro usmjerene ka forenzici mobilnih uređaja, a samim time i bespilotnim zrakoplovima.

Sukladno tome u ovome poglavlju bit će opisana referentna metodologija digitalne forenzike koje je razvijena od strane SANS instituta čija je uloga u svijetu digitalne forenzike i cyber sigurnosti ključna po pitanju edukacije i certificiranja u navedenom području.

Navedena metodologija sastoji se od 9 koraka, a oni su sljedeći:

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

Uvođenje

U prvom koraku uvođenje obuhvaća zapljenu, transport i predaju uređaja u forenzički laboratorij na ispitivanje. Prilikom pronalaska letjelice i samog procesa zapljene, potrebno je voditi opsežnu dokumentaciju sve do trenutka predaje uređaja u laboratorij.

Nadalje, kako bi se sačuvao lanac posjeda, potrebno je fotografirati sve dokaze i fotografije istih predati uz dokumentaciju forenzičkim stručnjacima u laboratoriju. Istražitelji određuju ciljeve istrage te tako postavljaju zahtjeve forenzičkim stručnjacima koji moraju biti ispoštovani, pritom pazeći na lanac posjeda dokaza prilikom rada s dokazima slučaja.

Identifikacija

Prilikom identifikacije forenzički stručnjaci moraju poznavati zakonsku regulativu i isto tako ispoštovati ono što je zatraženo sudskim nalogom i ne prekršiti lanac posjeda dokaza kao niti raditi nikakve nedozvoljene radnje tijekom trajanja istrage. Od forenzičkih stručnjaka zahtijeva se dobro poznavanje dokaznih materijala, odnosno zaplijenjenih uređaja kako bi mogli pronaći sve potencijalne elektroničke dokaze kako bi istima pristupili.

Identifikacijom dokaza, u ovom slučaju elektroničkih uređaja (bespilotnu letjelicu i mobilni uređaj), moguće je odrediti točan tip, odnosno model uređaja. Mobilni uređaj kao i bespilotnu letjelicu moguće je identificirati prema već određenim identifikatorima poput:

- ESN (engl. *Equipment Serial Number*)
- MEID (engl. *Mobile Equipment Identifier*)
- IMEI (engl. *International Mobile Equipment Identity*)
- ICCID (engl*. Integrated Circuit Card Identification Number*)
- MSISDN (engl. *Mobile Station International Subscriber Directory Number*)

Kako bi identificirali mobilni uređaj, moguće je prilikom povezivanja uređaja na forenzički alat saznati podatke poput proizvođača uređaja, model i ostale podatke.

Priprema

Problemi i poteškoće postoje u svakome poslu pa tako i u digitalnoj forenzici. Kako potreba za provođenjem forenzičke istrage ne poznaje vrijeme, a ni mjesto, potrebno je uvijek biti spreman i odgovoriti na izazov istrage. Vrijeme reakcije na incident ključno je, stoga je poželjno uvijek biti spreman kako bi mogli što prije reagirati i prikupiti digitalne dokaze. Kako bi osigurali što ispravniji pristup prikupljanja digitalnih dokaza i dokumentiranja, koristi se kontrolni popis.

Uobičajeni kontrolni popis sadrži, [31]:

- datum i vrijeme
- ime i prezime, kontakt osobe koja je pristupila incidentu
- opis otkrića incidenta
- ugrožene stavke sustava (hardver, operativni sustav, lokacija uređaja, mrežne informacije)
- poduzete radnje
- ostala razmatranja, poput pravnih i regulatornih aspekta incidenta

Kako bi forenzički stručnjaci mogli provesti istragu u cijelosti, prijeko su im potrebni alati o kojima je potrebno voditi stalnu brigu. Stalna briga podrazumijeva brigu o ispravnosti hardvera (alata), pribavi kablova za povezivanje uređaja i prijenos podataka, ali i brigu o valjanosti licence forenzičkog softvera. Osim navedenog, prilikom pripreme potrebno je i odrediti, odnosno odabrati ispravnu metodologiju koja će biti korištena u procesu istrage.

Izolacija

Na samom početku pronalaska mobilnog uređaja ili bespilotnog zrakoplova potrebno je provesti izolaciju. Izolacijom uređaja i zrakoplova sprječava se bilo kakav utjecaj na dokaze, izmjena dokaza ili brisanje kao i upravljanje istim uređajima. Ovaj proces mora biti konstantan tijekom cijele istrage u slučaju da je uređaj uključen, što znači od prikupljanja do završetka istrage.

Tehnike izolacije koje koristi ispitivač zbog sprječavanja gubitaka podataka ili narušavanja integriteta podataka potrebno je testirati na svim frekvencijama s kojima su se susrele tijekom ispitivanja. Neke od tehnika izolacije uređaja su folije, vreće, torbe, ali i zasebno izolirane sobe prema načelu Faradayevog kaveza. Osim navedenog, moguće je koristiti i blokatore signala (engl. *Jammer*).

Bitno je napomenuti da prilikom izolacije mobilnog uređaja dolazi do problema iznadprosječnog trošenja baterije uređaja jer uređaj pokušava uspostaviti vezu s mrežom. Zbog navedenog problema potrebno je osigurati valjano napajanje za uređaj ili postaviti uređaj u način zrakoplovnog moda.

Procesiranje

Procesiranje u forenzici označava početak ekstrakcije podataka iz uređaja, gdje se prvobitno uklanja vanjska memorija (memorijska kartica) te SIM kartica. Podatci vanjske memorije i SIM kartice su dohvatljivi i zbog svog sadržaja mogu igrati bitnu ulogu u sudskom procesu. Nakon navedenog, potrebno je provesti ekstrakciju podataka s uređaja koristeći se raznim alatima, poželjno je koristiti što veći broj alata kako bi pronašli što veći broj podataka.

Verifikacija

Prilikom izvođenja svake forenzičke istrage važno je osigurati lanac očuvanja dokaza, tj. spriječiti bilo kakvu izmjenu podataka na uređaju. Očuvanje izvornog digitalnog dokaza postiže se verifikacijom.

Jedan od načina verifikacije podataka je usporedba izvornih podataka s uređaja te podataka koji su dohvaćeni s uređaja. Drugi način verifikacije moguće je izvršiti korištenjem forenzičkih alata, gdje se izvodi verfiikacija *hash* algoritmom. Usporedbom *hash* vrijednosti izvornih i dohvaćenih podataka, može se utvrditi integritet podataka, [32].

Dokumentiranje

Razvijene organizacijske vještine i vođenje točnih bilješki tijekom forenzičke istrage izuzetno su bitne osobine forenzičkog stručnjaka jer je dokumentacija u ovoj grani važna kako bi mogli osigurati lanac posjeda dokaza, ali i ukoliko je potrebno, svjedočiti na sudu. Dokumentiranje digitalne forenzičke istrage obavlja se tijekom cijelog procesa i sastoji se od velikog broja bilješki.

Prema izvoru [33], imamo pet razina dokumentacije koje čine i moraju biti opisane u svakom slučaju, a to su:

- opća dokumentacija slučaja - dokumentacija vođena od samog početka istrage
- proceduralna dokumentacija - uključuje opis učinjenih koraka, opis cjelokupne procedure, korištene alate
- procesna dokumentacija - sastoji se od zapisa pronađenih dokaza, mjesta istragu, korištenih alata uz detaljan opis
- vremenska crta slučaja
- lanac posjeda dokaza

Prezentacija

Nakon završetka svih prethodnih procesa i opsežnog i pravilnog dokumentiranja potrebno je rezultate, kao i oporavljene podatke, prezentirati u sudskom procesu na način koji je razumljiv i potpuno jasan osobama koje nemaju znanje o područje digitalne forenzike. To znači da svi dokazi moraju biti što jednostavniji, ali i vizualno prikazani zbog boljeg razumijevanja istrage. Prezentacija može biti predana u digitalnom ili pisanom obliku.

Arhiviranje

Arhiviranje predstavlja posljednji proces svake forenzičke istrage i obuhvaća pohranu odnosno čuvanje dokumentacije slučaja. Arhiviranje dokumentacije je nužno, jer postoji mogućnost da će ista biti ponovno zatražena iako je sudski proces završio zbog mogućih naknadnih žalbi ili ponovnog sudskog procesa. Također, dokumentacija može biti korisna u novim slučajevima kako bi pomogla i olakšala proces istrage.

4.2. Postupci i metode ekstrakcije podataka

Ekstrakcija podataka predstavlja proces prikupljanja bitnih dokaza iz nekoliko različitih vrsta medija za pohranu kako bi se dobiveni dokazi mogli obraditi, pohraniti te kasnije analizirati. Kako bi došli do podataka koji se nalaze na bespilotnom zrakoplovu, kontroleru, ali i mobilnom uređaju nužno je pažljivo izvršiti proces ekstrakcije podataka. Vrijeme trajanje ekstrakcije podataka s bespilotnog zrakoplova ovisi o sadržaju, odnosno o količini podataka. Na slici 8 prikazan je omjer brzine

obavljanja ekstrakcije podataka i količine dobivenih podataka. Ručna ekstrakcija pripada najbržoj metodi ekstrakcije podataka, ali prema količini ekstrahiranih podataka nije ni blizu količini dokaza koju daje neka od fizički invazivnih metoda.



Slika 8. Usporedba brzine ekstrakcije i količine dobivenih podataka, [34]

Postoje razne metode ekstrakcije podataka, od onih jednostavnijih kojima se prikupljaju samo nužni podaci, a samim time takva ekstrakcija ne zahtijeva puno vremena, do onih kompliciranijih ekstrakcija za koje je potrebno puno više vremena i specijaliziranijih alata. Takve ekstrakcije namijenjene su posebnim službama kao što su vojska, policija, obavještajne agencije i tvrtke čija je primarna djelatnost digitalna forenzika.

4.2.1. Ručna ekstrakcija

Ručna ekstrakcija podataka provodi se samo u slučaju ako je mobilni uređaj otključan i uključen, jer je potrebno koristiti mobilni uređaj, odnosno sučelje za pregledavanje postavki uređaja, datoteke pohranjene na njemu, tj. cjelokupni sadržaj koji je dostupan korisniku. Za vrijeme provođenja ručne ekstrakcije potrebno je fotografirati svaki korak kako bi se potkrijepili svi rezultati u dokumentaciji. Ovakva ekstrakcija je izrazito lagana za provođenje i kao takva ne zahtijeva osposobljavanje za njezino izvođenje.

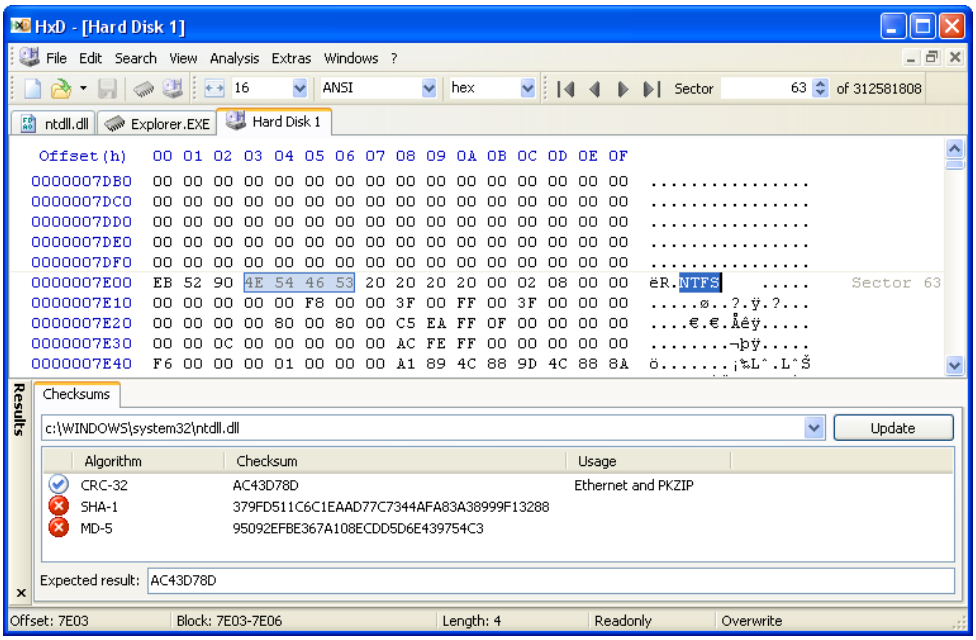
4.2.2. Logička ekstrakcija

Za potrebe provođenja logičke ekstrakcije nužno je povezivanje mobilnog uređaja s forenzičkom radnom stanicom putem USB kabela, infracrvenog ili Bluetooth veze. Nakon uspješnog spajanja, forenzička radna stanica automatizirano pokreće proces ekstrakcije komunikacijom s operativnim sustavom uređaja. Željeni podatci s mobilnog uređaja ekstrahiraju se na forenzičku radnu stanicu ili po potrebi na vanjski medij za pohranu (npr. prijenosni tvrdi disk) za potrebe analize.

Ono što odlikuje ovu metodu ekstrakcija je brzina izvođenja ekstrakcija, ali i jednostavnost korištenja. Logičkom ekstrakcijom nije moguće oporaviti izbrisane podatke. Također, postoji opasnost od nenamjerne izmjene podataka, čime se narušava integritet dokaza, [35].

4.2.3. Hex dump

Hex dump, kao i logička ekstrakcija, zahtijeva povezivanje uređaja na forenzičku radnu stanicu kako bi fizički došli do sirovih podataka pohranjenih na memoriji uređaja. Nakon povezivanja uređaja na radnu stanicu dolazi do prijenosa kodova koji se sastoje od seta instrukcija. Set instrukcija omogućuje preuzimanje cijele memorije uređaja i njezin prijenos na radnu stanicu, [36].



Slika 9. Prikaz heksadecimalnog zapisa pomoću Hex preglednika, [37]

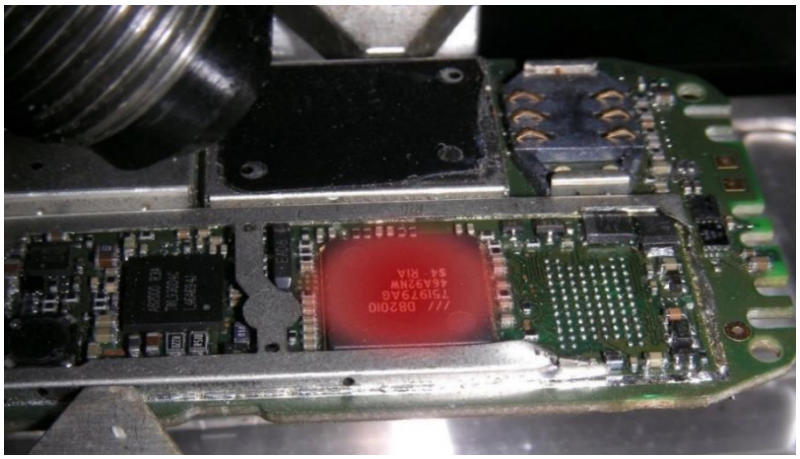
Podatci nakon logičke ekstrakcije mogu biti u binarnom obliku, stoga se koriste alati poput Oxygen Forensics Detective ili UFED Physical Analyzer kako bi pretvorili zapis i na zaslonu vidjeli vrijednosti.

Hex preglednici omogućavaju pregled, ali i pretraživanje memorijskih heksadecimalnih zapisa (slika 9).

4.2.4. Chip-off

Chip-off predstavlja invazivnu metodu ekstrakcije digitalnih podataka i uključuje fizičko uklanjanje flash memorijskog čipa iz uređaja i dobivanje podataka. Prvotno se memorijski čip odvaja s matične ploče uređaja korištenjem lemilice ili kemijskih sredstava te se nakon odvajanja postavlja na čitač čipa pomoću kojeg se vrši čitanje, odnosno izdvajanje podataka.

Kako se za odvajanje čipa koristi lemilica ili neki alat za zagrijavanje čipa, nužno je biti oprezan jer vrlo lako može doći do oštećenja memorijskog čipa, što u konačnici može rezultirati gubitkom podataka. Ova metoda se koristi samo onda kada nije moguće provesti druge metode.



Slika 10. Primjena Chip-off metode zagrijavanjem čipa uređaja, [38]

Postupak Chip-off metode sastoji se od četiri koraka, [39]:

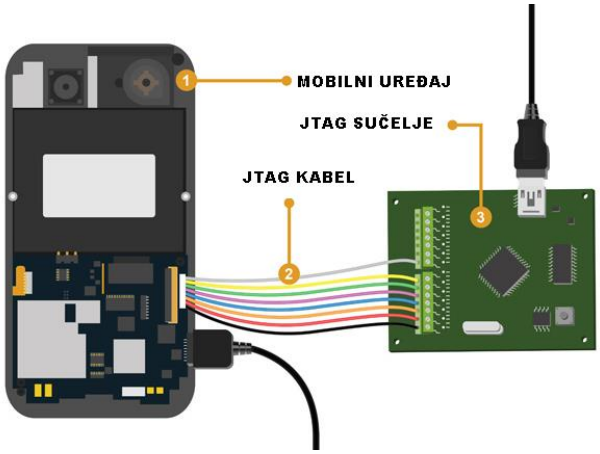
- fizičko uklanjanje čipa korištenjem lemilice ili posebnih kemijskih sredstava
- čišćenje i popravljanje čipa
- ekstrakcija podataka s čipa
- analiziranje dobivenih podataka s čipa forenzičkim alatima.

4.2.5. Micro read

Ekstrakcija podataka micro read metodom obuhvaća pregled NAND ili NOR memorijskog čipa koristeći se elektronskim mikroskopom. Kao i prethodna metoda, ova metoda se koristi samo onda kada ostale metode nije moguće provesti iz nekog razloga ili iste ne daju rezultate, [40]. Ovakva vrsta ekstrakcije izrazito je kompleksna i spora te se rijetko provodi.

4.2.6. Ekstrakcija podataka JTAG metodom

JTAG (engl. *Joint Action Test Group*) metoda omogućuje forenzičkim istražiteljima da fizički „steknu“ uređaj. Fizička ekstrakcija omogućuje nastanak kompletnog *image* sustava, gdje se ne kopira sustav datoteka. Provođenjem ovakve metode forenzičari ostvaruju pregled svih datoteka, uključujući i one izbrisane koje bi bile propuštene nižim hijerarhijskim ekstrakcijama.



Slika 11. JTAG ekstrakcija podataka s mobilnog uređaja, [41]

JTAG metoda zahtijeva izravni pristup memorijskom čipu uređaja, što obuhvaća invazivne, ali i destruktivne postupke za koje je potrebno znanje, pažnja i strpljivost kako se čip ne bi oštetio. Provođenje ove metode obuhvaća povezivanje vodova na posebni priključak za testiranje na matičnoj ploči uređaja. Na taj način moguće je ekstrahirati podatke s memorijskog čipa izravno na forenzičku radnu stanicu (slika 11), [42].

4.3. Izvori podataka sustava bespilotnog zrakoplova

Kako je već prethodno rečeno, na bespilotne zrakoplove možemo gledati kao i na mobilne uređaje. Prema tome, može se reći da se svakom uporabom bespilotnog zrakoplova i cijelog sustava nastaju dokazi. Prilikom provođenja forenzičke analize sustava bespilotnih zrakoplova bitno je poznavati izvore podataka kao i tipove podataka koji mogu biti korisni u sudskom procesu.

Kao i kod mobilnih uređaja, fotografije i video zapisi nastali korištenjem bespilotnog zrakoplova mogu biti izrazito bitni dokazi. Ponajviše jer navedeni dokazi mogu biti obogaćeni s puno detalja, obuhvatiti kretanja ljudi kao i vozila, pružiti visoku kvalitetu fotografije kao i video zapisa te vrijeme događaja.

Osim glavnih dokaza, fotografija i video zapisa bespilotne letjelice pohranjuju puno više dokaza koji mogu biti od velike pomoći prilikom forenzičke istrage. Takvi dokazi obuhvaćaju razne log zapise, podatke senzora, povezivanja i ostalog. Ti podatci nestručnoj osobi nisu od koristi i stoga je bitno da forenzički stručnjak prilikom provođenja istrage obuhvati ekstrakciju svih podataka zrakoplova i prilikom analize izvrši uvid u iste kako bi iz tih podataka dobili najveći set korisnih podataka.

Multimedijski podatci (fotografije i video zapisi) su često glavni i krucijalni dokazi svake forenzičke istrage i prema tome forenzičkim stručnjacima oni predstavljaju prioritet prilikom ekstrakcije i analize. Količinski multimedijski podatci zauzimaju najveći dio pohrane svakog bespilotnog zrakoplova, a porastom kvalitete kamere i razlučivosti iste zahtjevi za pohranom su sve veći. Multimedijski podatci bespilotnog zrakoplova pohranjuju se u unutarnjoj pohrani samog zrakoplova, ali naravno ovisno prema modelu zrakoplova moguće je iste pohraniti na vanjsku memoriju (memorijsku karticu).

Metapodatci bespilotnog zrakoplova forenzičkim stručnjacima mogu dati uvid u bitne dokaze koji su nevidljivi običnom čovjeku. Ovakvi podatci nisu klasični podatci, nego su zapravo proširenje postojećih podataka gdje se sadržaj podataka obogaćuje dodatnim informacijama. Primjer metapodataka su: vrijeme, datum, lokacija, brzina, smjer, visina, napon baterija i razni drugi podatci zabilježeni senzorima.

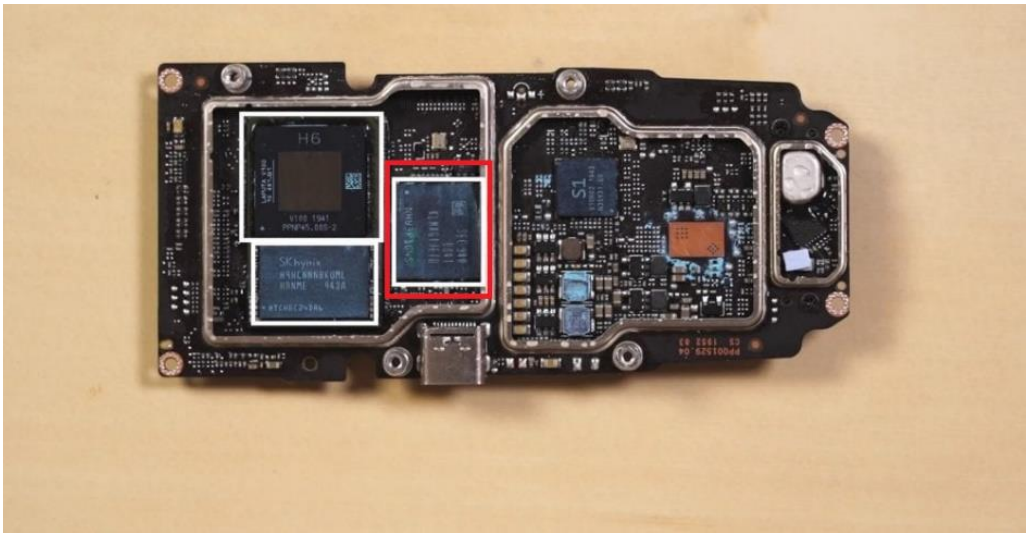
Određeni metapodatci zahtijevaju izrazito visoko poznavanje razumijevanja zapisa kako bi mogli iste interpretirati, no zahvaljujući modernim forenzičkim alatima moguće je dobiti uvid u iste u kratkom razdoblju.

Primjerice, log zapisi napona baterije bespilotnog zrakoplova mogu puno toga otkriti, ali od svih dostupnih alata na tržištu trenutno XRY jedini nudi mogućnost interpretacije navedenog zapisa. Podatci poput vremena, datuma, koordinata lokacije postali su standard i pomoću forenzičkih alata moguće je prikazati i interpretirati aktivnosti, odnosno letačke aktivnosti.

Porastom broj raznih senzora kao i dodataka koje je moguće dodati na bespilotne zrakoplove raste i broj podataka. Korištenjem dodataka nastaju podatci koji se prvotno prikazuju operatoru, ali isti se pohranjuju na uređaj. Forenzičkom stručnjaku provođenjem analize bit će moguće doći do dokaza koji senzor ili dodatak su korišteni, kada i gdje.

Prilikom provođenja forenzičke ekstrakcije podataka UAS potrebno izvršiti ekstrakciju podataka iz nekoliko izvora, a oni su, [43]:

- Unutarnja pohrana UAV
- Vanjska pohrana UAV (memorijska kartica)
- Kontroler
- Terminalni mobilni uređaj
- Zemaljska stanica
- Cloud platforma



Slika 12. Unutarnja pohrana bespilotnog zrakoplova DJI Mavic Air 2, [44]

Unutarnja i vanjska pohrana UAV

Unutarnja pohrana bespilotnih zrakoplova je prvotno uspostavljena od strane tvrtke DJI. Unutarnja pohrana bespilotnog zrakoplova služi za kratkotrajnu pohranu podataka koji su nastali tijekom korištenja i preporučljivo je nakon svakog leta izbrisati iste podatke. S forenzičkog stajališta to može biti loše jer se time gube podatci, ali postoji šansa za oporavak istih. Unutarnja pohrana svakog UAV nije ista, ona varira ovisno o samom proizvođaču, što je isto kao i kod mobilnih uređaja. Unutarnja memorija zrakoplova je proširiva vanjskom pohranom, odnosnom memorijskom karticom.

Provođenje ekstrakcije unutarnje pohrane također nije uobičajeno jer određeni modeli omogućavaju jednostavnu ekstrakciju koristeći kablove koji se spajaju na radnu stanicu i dron, dok kod nekih modela postoji potreba za korištenjem invazivnijih fizičkih metoda kako bi se došlo do samih podataka.

Za razliku od unutarnje pohrane, vanjska memorijska pohrana ne zahtijeva toliko invazivne metode prilikom ekstrakcije podataka. Podatci koji se pohranjuju na memorijskom čipu su multimedijski podatci i razni log zapisi poput koordinata, podataka o kontroleru, vremenskih zapisa i sl.

Prednost memorijske kartice je što za vrlo nisku cijenu proširuje memorijski kapacitet same letjelice i tako omogućuje stvaranje velike količine multimedijskih podataka kao i stvaranje dodatnih podataka koji mogu biti korisni u istrazi.

Kontroler

Kontroler prilikom provođenja forenzičke istrage može biti ključan dokaz, jer je isti taj kontroler korišten za upravljanje bespilotnim zrakoplovom i predstavlja isto što i ključ osobnog vozila, identifikator. Stoga kontroler može pomoći prilikom identifikacije zrakoplova.

Ovisno o izvedbi kontrolera, moguće je pronaći podatke vezane za prethodne letove kao i sve podatke o povezanom zrakoplovu kao što su serijski broj zrakoplova, mrežne oznake korištene prilikom povezivanja kontrolera i bespilotnog zrakoplova IP (engl. *Internet Protocol*) i MAC (engl. *Maedia Access Control*) adresu, SSID (engl. *Service Set Identifier*), informacije o Bluetooth povezivanju, te podatke o povezanim mobilnim uređajima s kontrolerom. Ukoliko je korišten i mobilni uređaj za upravljanje zrakoplovom moguće je doći do još više bitnih i korisnih podataka za istragu o čemu će biti više riječi u nastavku.

Pametni mobilni uređaj

Ukoliko dođe do pronalaska mobilnog uređaja koji je korišten za upravljanje zrakoplovom, provođenjem ekstrakcije podataka s istog uređaja moguće je doći do možebitnih podataka koje generira letačka aplikacija (npr. DJI GO 4). Mobilni uređaj pohranjuje multimedijske datoteke nastale uporabom letačke aplikacije kao i razne log zapise.

Budući da je mobilni uređaj odvojeni dio sustava bespilotnog zrakoplova, prilikom ekstrakcije podataka moguće je pronaći i podatke koji nisu interes same istrage poput podataka drugih aplikacija, korisničke račune i lozinke, IMEI i IMSI broj. Mobilni uređaj može pohranjivati podatke na unutarnjoj pohrani kao i na vanjskoj pohrani, odnosno memorijskoj kartici, ali i na SIM kartici.

Zemaljska stanica

Dohvaćanje podataka zemaljske stanice vrši se analizom stanice i svih njezinih komponenata forenzičkim alatima kako bi mogli dobiti sve bitne podatke i tako rekonstruirali događaj.

Cloud

Budući da sustav bespilotnih zrakoplova ima mogućnost pohrane podataka na cloud platformu, ista ta platforma forenzičkim stručnjacima predstavlja veliki interes. Cloud platforma sadrži veliki broj korisnih dokaza o cloud računu, modelu zrakoplova, povijesti leta i raznim metapodatcima. Kako bi forenzički stručnjaci pristupili cloud platformi, sve što je potrebno znati su korisničko ime i lozinka. Platforma DJI cloud ne koristi dvostruku provjeru autentičnosti, stoga forenzičkim stručnjacima ovakav izvor podataka ne predstavlja veliki izazov i moguće je vrlo lako izdvojiti podatke, [45].

5. Komparativna analiza mogućnosti alata usmjerenih bespilotnim zrakoplovima

Budući da izrada ovoga diplomskoga rada obuhvaća područje digitalne forenzike bespilotnih zrakoplova, za potrebe praktičnog dijela rada provedena je forenzička analiza sustava bespilotnog zrakoplova. DJI Mavic Air je bespilotni zrakoplov koji je korišten za izvršavanje letačkih aktivnosti, ali i za forenzičku analizu podataka. Letačke aktivnosti izvršene su na području Sveučilišnog kampusa Borongaj poštujući sve mjere koje su propisane za upravljanje ovim bespilotnim zrakoplovom. Nadalje, sam postupak ekstrakcije, ali i analize podataka izvršen je u Laboratoriju za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava Fakulteta prometnih znanosti pod vodstvom i mentorstvom dr. sc. Siniše Husnjak.

Kako stvarni forenzički procesi zahtijevaju detaljan opis cijelog procesa istrage od prikupljanja do izvještaja, tako će i u nastavku ovog poglavlja proces biti opisan tim redoslijedom.

Na samom početku izvođenja praktičnoga rada bilo je potrebno provesti određene predradnje kako bi provođenje forenzičke analize dalo zadovoljavajuće rezultate. Osim bespilotnog zrakoplova, za potrebe dodatnog upravljanja i iskorištavanja mogućnosti letjelice korišten je pametni mobilni uređaj Xiaomi Redmi Note 4X baziran na Android operativnom sustavu. Navedeni mobilni uređaj je prije povezivanja s zrakoplovom nekoliko puta vraćen na tvorničke postavke kako bi svi podatci nastali prethodnim korištenjem nestali.

Vanjska pohrana (memorijska kartica) uređaja je formatirana nekoliko puta. Kako bi dodatno olakšali dohvaćanje podataka i samim time dobili bolje rezultate, nad pametnim mobilnim uređajem izvršen je proces tzv. *Rootanja*. *Rootanje* je proces pomoću kojega je moguće ostvariti privilegirani nadzor nad samim uređajem, čime je omogućena potpuna kontrola nad uređajem. Time je moguće raditi razne izmjene koje običnim Android korisniku nisu dostupne, [46]. Prilikom *rootanja* uređaja brišu se svi postojeći podatci pa je prethodno potrebno napraviti backup. *Rootanje* je izvršeno pomoću Magisk alata otvorenog koda te je na samom kraju instaliran Magisk Manager kako bi se omogućila potpuna funkcionalnost uređaja, a da se pritom ne izgubi pristup Google Play Store-u.

Za upravljanje i ostvarivanje dodatnih funkcionalisti zrakoplovom DJI Mavic Air potrebno je koristiti DJI GO 4 aplikaciju na mobilnom uređaju. Navedena aplikacija je izuzetno bitna i podatci koji nastaju korištenjem iste značajno pomažu prilikom forenzičke analize.

Nakon instaliranja aplikacija na uređaju, prije samog leta napunjene su baterije zrakoplova i kontrolera te je na zrakoplovu DJI Mavic Air izvršeno postavljanje na tvorničke postavke, kao i formatiranje vanjske i unutarnje pohranu.

Povezivanje mobilnog uređaja i kontrolera je izvršeno pomoću USB žičane veze te je pritom obavljeno ažuriranje *firmware* bespilotnog zrakoplova. Kako bi mogli letjeti, bilo je potrebno izvršiti kalibraciju bespilotnog zrakoplova, konkretno IMU (engl. *Inertial Measurement Unit*), ali i kompasa. Nakon ispunjenih uvjeta, let je započeo. Letačke aktivnosti odvijale su se na području kampusa Borongaj gdje nema drugih letjelica i objekata. Prilikom letačkih aktivnosti iskorištene su 3 baterije te je ukupan let trajao 47 min. U tome razdoblju načinjeno je nekoliko fotografija i video zapisa gdje se lokacija pohrane istih mijenjala za potrebe istraživanja diplomskog rada.

Nakon završetka leta, mobilni terminalni uređaj postavljen je u zrakoplovni način rada kako bi očuvali lanac posjeda dokaza i tako zaštitili uređaj od bilo kakve kompromitacije dokaza.

Za potrebe forenzičke analize i ekstrakcije podataka zrakoplova, ali i mobilnog uređaja bila je korištena prijeko potrebna oprema i alati.

Korišten hardver:

- DJI Mavic Air
- DJI kontroler
- Xiaomi Redmi Note 4X
- USB kabel (punjenje mobilnog uređaja i kontrolera)
- Punjač i baterije za DJI Mavic Air
- UFED Touch 2
- USB kablovi za povezivanje uređaja na UFED Touch 2
- Forenzička radna stanica
- Medij za pohranu-tvrdi disk

Korišten softver:

- DJI GO 4 aplikacija
- UFED Physical Analyzer
- Oxygen Forensics Detective
- DatCon
- CsvView

Većinu gore navedene opreme, ali i forenzičke alate, omogućio je Laboratorij za sigurnost i forenzičku analizu informacijskog komunikacijskog sustava. Iz navedenog razloga odluka je prvenstveno pala na odabir Cellebrite UFED Touch 2 kao glavni alat forenzičke istrage.

UFED Touch 2, kako je već prethodno opisano, je hardverski alat tvrtke Cellebrite koji omogućava ekstrakciju podataka mobilnih uređaja, bespilotnih zrakoplova (trenutno samo određene modele zrakoplova tvrtke DJI i Parrot) i GPS uređaja.

Prednost je i mogućnost kloniranja SIM kartice, ali i oporavak izbrisanih podataka koji je kasnije moguće analizirati pomoću UFED Physical Analyzer-a na forenzičkoj radnoj stanici.

Zbog raznovrsnosti gore navedenih uređaja Cellebrite isporučuju posebne USB kablove koji omogućavaju povezivanje uređaja na UFED Touch 2.

Osim samog UFED Touch 2, UFED Physical Analyzer je nužan kako bi mogli provoditi analizu podataka nastalih ekstrakcijom, te iste dekodirati i naposljetku kreirati izvještaj.

Za potrebe usporedbe alata, odabir alata nije bio jednostavan jer je prisutna problematika podrške bespilotnih zrakoplova, odnosno DJI Mavic Air nije podržan i nije moguće izvršiti ekstrakciju, ali ni analizu podataka. Stoga je odluka pala na alat tvrtke Oxygen Forensic, Oxygen Forensics Detective. Oxygen Forensics Detective predstavlja softversku forenzičku platformu namijenjenu ekstrakciji, dekodiranju i analizi podataka iz nekoliko vrsta izvora:

- Mobilni uređaji
- IoT uređaji
- UICC kartice
- Memorijske kartice
- Backup uređaja
- Cloud usluge
- Bespilotni zrakoplovi

Zahvaljujući inovativnoj tehnologiji koja je razvijena za potrebe alata omogućava zaobilaženje zaključanih zaslona uređaja, otkrivanje lozinke, ekstrakciju podataka zaštićenih aplikacija kao i oporavak izbrisanih datoteka.

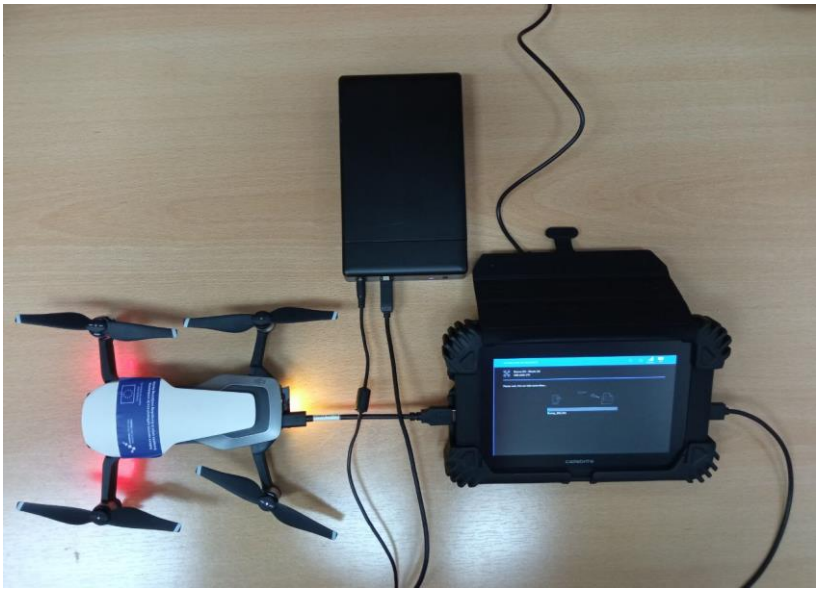
Oxygen Forensics Detective omogućava provedbu fizičke ekstrakcije podataka bespilotnog zrakoplova i prikaz GPS lokacija putanje leta kao i prikaz vremenskog tijeka leta kroz zasebno sučelje ovoga alata. Ovaj alat također omogućava istražiteljima uvoz log zapisa zrakoplova (.DAT datoteka) za potrebe vizualizacije lokacija i praćenja putanje bespilotnog zrakoplova.

Važno je naglasiti da ovaj alat omogućava i fizičku ekstrakciju unutarnje i vanjske pohrane bespilotnih zrakoplova tvrtke DJI kao i prikaz podataka letačkih aplikacija s mobilnog uređaja. Moguće je izvršiti ekstrakciju podataka s cloud servisa poput DJI Cloud i SkyPixel, [47].

Iako ovaj alat nema direktnu mogućnost ekstrakcije podataka iz zrakoplova DJI Mavic Air, pruža mogućnost za uvoz i analizu log zapisa zrakoplova i podataka letačke aplikacije i uvoz UFED datoteke i analizu iste. UFED Touch 2 kao i Oxygen Forensics Detective odabrani su za ekstrakciju i analizu podataka mobilnog uređaja.

5.1. Ekstrakcija podataka s DJI Mavic Air

Proces ekstrakcije i analize podataka s bespilotnog zrakoplova DJI Mavic Air izvršen je u laboratoriju. Prvo je započeta ekstrakcija spajanjem zrakoplova s UFED Touch 2. Povezivanje zrakoplova i UFED Touch 2 vrši se pomoću posebnog kabela (USB Cabel 170), a moguće je izvršiti ekstrakciju datotečnog sustava i fizičku ekstrakciju. Za potrebe spremanje *image* datoteka zrakoplova korišten je vanjski tvrdi disk koji je potrebno spojiti na UFED Touch 2. Isti taj *image* kasnije se analizira na forenzičkoj radnoj stanici. Važno je napomenuti da UFED Touch 2 dodjeljuje *hash* vrijednost *image* datoteci, konkretno SHA-256.



Slika 13. Proces ekstrakcije podataka pomoću UFED Touch 2

Prilikom provođenja ekstrakcije nužno je voditi brigu o napunjenosti baterije zrakoplova, stoga je najbolje napuniti bateriju i tek tada započeti s ekstrakcijom. Prilikom ekstrakcije podataka, potrošena je polovina kapaciteta baterije.

Provođenje ekstrakcije podataka s bespilotnog zrakoplova DJI Mavic Air pomoću alata Oxygen Forenscis Detective nije bilo moguće jer navedeni zrakoplov nije podržan. Ali budući da ovaj alat ima mogućnost analize *dump* datoteke, odnosno *image*-a zrakoplova, *image* je učitan u Oxygen Forenscis Extractor i nakon toga izvršena je analiza.

Budući da je moguće povezati bespilotni zrakoplov na računalo i tako pristupiti datotekama koje se nalaze na njemu isto je i učinjeno. Pronađene su i pohranjene multimedijske datoteke, ali i datoteke s raznim ekstenzijama koje je moguće analizirati i tako doći do dodatnih informacija.

Datoteke vidljive u DCIM direktoriju:

- Fotografije-JPG format-DJI_xxxx.JPG (npr. DJI_0033.JPG)
- Video zapis-MP4 format-DJI_xxxx.MP4 (npr. DJI_0074.MP4)
- Subrip-SRT format-DJI_xxxx.SRT (npr. DJI_0074.SRT)

Veliki je broj fotografija pohranjenih na oba medija za pohranu, gdje je u prosjeku jedna fotografija kapaciteta 5 MB, količina video zapisa je manja, ali oni su ti koji zauzimaju najviše mjesta u pohrani. Datoteke formata .SRT su datoteke vezane uz nastale video zapise, a sadrže samo tekst koji se koristi zajedno s podacima o videozapisu. SRT datoteke ne sadrže nikakve video ili audio podatke, [48].

Kontroler bespilotnog zrakoplova DJI Mavic Air uz mobilni uređaj je izuzetno bitan i ključan dokaz i očekivano je da će na njemu biti pronađeni dokazi prilikom povezivanja na UFED Touch 2, Oxygen Forensics Detective, ali i na forenzičku radnu stanicu. Unatoč uloženom silnom naporu i pokušajima dolaska do dokaza na kontroleru, dokazi nisu pronađeni, odnosno niti jedan uređaj nije prepoznao kontroler. I upravo zbog toga u diplomskom radu kontroler kao dokazni uređaj neće biti dio istraživanja.

5.2. Ekstrakcija podataka mobilnog uređaja

Provođenje ekstrakcije podataka s mobilnog uređaja pomoću alata UFED Touch 2 doista je slično prethodno izvršenoj ekstrakciji podataka s bespilotnog zrakoplova. Za povezivanje mobilnog uređaja i UFED Touch 2 uređaja korišten je kabel T-100. Važno je napomenuti da je nužno izvršiti izolaciju mobilnog uređaja prije provođenja ekstrakcija, kako bi spriječili bilo kakvo zlonamjerno udaljeno modificiranje ili brisanje podataka kao i nastanak novih podataka prilikom povezivanja na mrežu. Izolacija uređaja izvršena je postavljanjem uređaja u zrakoplovni način rada. Tijekom korištenja mobilnog uređaja za upravljanje zrakoplovom SIM kartica i memorijska kartica nalazile su se u uređaju te je izvršena ekstrakcija podataka s memorijske kartice koja je prethodno formatirana.

Kako bismo dobili maksimalne rezultate, bilo je potrebno na mobilnom uređaju u postavkama omogućiti *USB debugging mode*, prilagoditi postavke razvojnog inženjera kao i prijenos podataka s mobilnog uređaja na UFED Touch 2. Prilikom povezivanja uređaja, UFED Touch 2 prepoznao je model uređaja te prikazao bitne informacije o istom poput verzije operativnog sustava, broj instaliranih aplikacija, IMEI, količinu pohranjenog sadržaja i ostalo. Osim navedenog, alat je prepoznao da je uređaj root-an.



Slika 14. Ekstrakcija podataka mobilnog uređaja pomoću uređaja UFED Touch 2

U sljedećem koraku je otkriveno kako UFED Touch 2 ne podržava velik broj ekstrakcija podataka s mobilnog uređaja koji je korišten za upravljanje bespilotnim zrakoplovom. Podržana je napredna logička ekstrakcija koja predstavlja neinvazivnu metodu ekstrakciju, ali ne daje puno rezultata kao primjerice fizička ekstrakcija. Prije same potvrde o početku ekstrakcije, na zaslonu UFED Touch 2 moguće je odabrati izvore ekstrakcije uređaja, u ovom slučaju odabrani su uređaj, SIM kartica i memorijska kartica. Proces napredne logičke ekstrakcije je trajao 5 minuta i u navedenom procesu nužno je bilo nekoliko puta potvrditi na zaslonu mobilnog uređaja dozvoljena za instalaciju i pristup uređaju od strane UFED Touch 2 uređaja.

Uz UFED Touch 2 za potrebe ekstrakcije podataka s mobilnog uređaja korišten je i Oxygen Forensics Detective. Oxygen Forensics Detective je prethodno instaliran, postavljen na forenzičku radnu stanicu i isti je korišten za analizu podataka bespilotnog zrakoplova. Nasuprot UFED Touch 2, Oxygen Forensics Detective podržava naprednu logičku, kao i fizičku ekstrakciju podataka s mobilnog uređaja.

Povezivanje mobilnog uređaja na forenzičku radnu stanicu vrši se pomoću USB podatkovnog kabela, preporučljivo je koristiti originalni kabel proizvođača mobilnog uređaja kako ne bi došlo do problema prilikom ekstrakcije, odnosno nemogućnosti provođenja iste.

Netom prije početka ekstrakcije, na zaslonu forenzičke radne stanice Oxygen Forensics Extractor napominje kako je potrebno učini sljedeće:

- Napuniti bateriju uređaja
- Otključati uređaj
- Omogućiti zrakoplovni način rada
- Omogućiti *USB debuging mod*
- Prihvatiti RSA ključ
- Omogućiti rad uređaja na način da se zaslon ne isključuju

Nakon uspješnog povezivanja uređaja na stanicu, Oxygen Forensics Extractor prikazuje podatke o uređaju kao što su model, IMEI, verzija softvera i hardvera. U sljedećem koraku potrebno je odabrati dodatne mogućnosti ekstrakcije koje nudi ovaj alat i nakon toga ekstrakcija podataka započinje:

- Odabir *hash* algoritama
- Mogućnost oporavka izbrisanih datoteka
- Zapostavljanje podataka
- Napredna analitika
- Pretraga prema ključnim riječima i sl.

Kao i u slučaju bespilotnog zrakoplova, mobilni uređaj spojen je na forenzičku radnu stanicu kako bi proveli ručnu ekstrakciju podataka. Svi dostupni podatci mobilnog uređaja pohranjeni su na tvrdi disk radi daljnje analize podataka.

5.3. Analiza ekstrahiranih podataka

U ovom potpoglavlju bit će opisani rezultati analize ekstrakcije podataka bespilotne letjelice i mobilnog uređaja dobivenih ručnom pretragom uređaja kao i korištenjem forenzičkih alata.

5.3.1. Analiza podataka ekstrahiranih alatom Cellebrite UFED Touch 2

Provođenjem ekstrakcije datotečnog sustava i fizičke ekstrakcije pomoću UFED Touch 2 uređaja nastala su dva zasebna direktorija na tvrdom disku koja se sastoje od datoteka .UFDX i .UFD formata. Koristeći Physical Analyzer prethodno navedene datoteke je potrebno učitati i dekodirati kako bi u konačnici dobili izvještaj koji jasno i jednostavno vizualizira sve što je pronađeno na uređaju.

U nastavku, dobiveni rezultati bit će opisani prikazom izvještajem, ali i slikama sučelja alata Physical Analyzer.

DJI Mavic Air-ekstrakcija datotečnog sustava

Na samom početku kreiranog izvještaja u sažetku navedene su informacije o ekstrakciji poput vremena početka i završetka ekstrakcije, datum ekstrakcije, tko je izvršio ekstrakciju, mjesto, naziv uređaja nad kojim je provedena ekstrakcija, datotečni sustav i sl. (slika 15). Izvještaj ekstrakcije datotečnog sustava sastoji se od 11 stranica.

Summary

UFED Physical Analyzer version	7.33.0.30
Report creation time	20.1.2021. 12:57:14 +01:00
Time zone settings (UTC)	Original UTC value
Examiner name	Petar Majić
Location	Zagreb
Case number	2
Case name	Mavic Air D

Source Extraction

File System	
Extraction start date/time	18.1.2021. 10:48:03(UTC+1)
Extraction end date/time	18.1.2021. 11:07:45(UTC+1)
Unit identifier	7211345
UFED version	7.40.0.85
Internal version	7.40.0.85
Selected manufacturer	Drone
Selected device name	DJI - Mavic Air
Machine name	TOUCH2-7211345
Connection type	Cable No. 170
Extraction type	File System
Extraction ID	C47F8C3D-CD38-4715-8D4F-5D9E573586E6
Extraction (UFD) file data integrity	Not available

Slika 15. Sažetak informacija o ekstrakciji datotečnog sustava

Datotečnom ekstrakcijom ukupno je pronađeno 123 datoteke, od toga:

- 3 arhivske datoteke
- 13 konfiguracijskih datoteka
- 1 baza podataka
- 11 slika
- 95 tekstualnih datoteka

Dohvaćene 3 arhivske datoteke su NOTICE.html.gz, otacerts.zip i recovery-resource.dat, gdje posljednja datoteka predstavlja recovery datoteku. Konfiguracijske datoteke, kako ime i samo kaže, čine konfiguracijski podatci bespilotnog zrakoplova za mrežno povezivanje putem WiFi, postavke kamere i FTP protokol.

Multimedijski podatci, odnosno slike koje su pronađene prilikom datotečne ekstrakcije nisu produkt korištenog senzora kamere tijekom leta, nego su to slike sistemskih ikona Android operativnog sustava. Tekstualne datoteke čine količinski veliki broj dohvaćenih podataka, a riječ je o log zapisima vezanih uz konfiguraciju zrakoplova, ali i prisutnim senzorima.

Interpretacija log zapisa je izuzetno zahtjevna i bez velikog znanja interpretacija istih nije izvediva. Log zapisi letjelica predstavljaju skriveno blago jer je u tekstualnom zapisu zapisano mnogo toga što može biti korisno za istragu.

Primjerice, vrijednosti padova napona baterije mogu pomoći stručnjacima u vještačenju ili otkrivanju informacija vezanih uz operatera zrakoplova. Jedina pronađena baza podataka je baza dynamic.db koji sadrži zapis u heksadecimalnom obliku (slika 16).



Slika 16. Prikaz sadržaja baze podataka

DJI Mavic Air-fizička ekstrakcija

Kao i za prethodnu ekstrakciju, kreiran je izvještaj fizičke ekstrakcije gdje su na 27 stranica izvještaja ispisane informacije o ekstrakciji. Za razliku od prethodnog izvještaja, ovaj izvještaj sadržava lokacijske podatke multimedijskih datoteka koje su nastale korištenjem kamere zrakoplova. Na samom početku izvještaja vidljivo je kako je korišten veći broj dodataka prilikom fizičke ekstrakcije u odnosu na datotečnu ekstrakciju.

Summary

UFED Physical Analyzer version	7.33.0.30
Report creation time	20.1.2021. 12:42:29 +01:00
Time zone settings (UTC)	Original UTC value
Examiner name	Petar Majić
Location	Zagreb
Case number	1
Case name	Mavic Air

Source Extraction

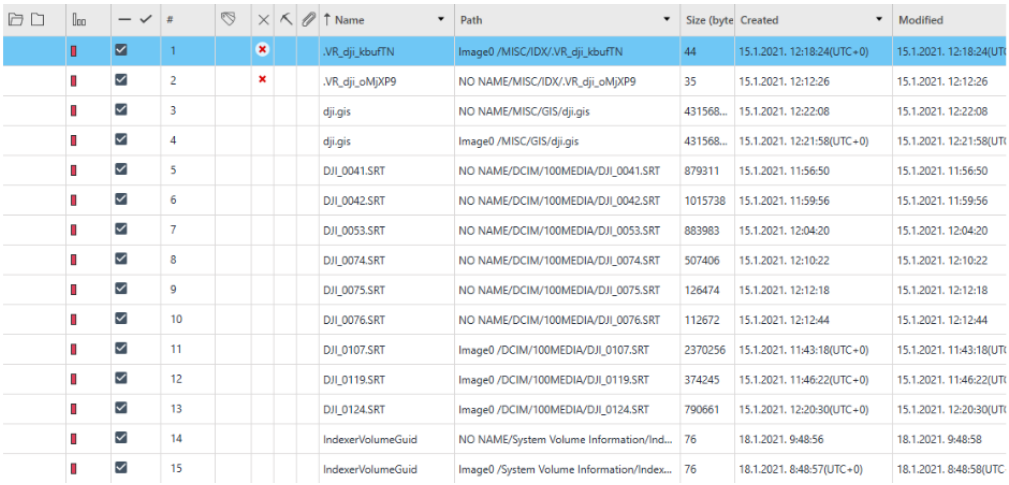
Physical	
Extraction start date/time	18.1.2021. 9:50:40(UTC+1)
Extraction end date/time	18.1.2021. 10:43:50(UTC+1)
Unit identifier	7211345
UFED version	7.40.0.85
Internal version	7.40.0.85
Selected manufacturer	Drone
Selected device name	DJI - Mavic Air
Machine name	TOUCH2-7211345
Connection type	Cable No. 170
Extraction type	Physical
Extraction ID	635F9DBB-FD76-4E4B-B928-1F5F31EE2127
Extraction (UFD) file data integrity	Not available

Slika 17. Sažetak informacija o fizičkoj ekstrakciji

Fizičkom ekstrakcijom podataka bespilotnog zrakoplova, otkrivene su sljedeće datoteke:

- 15 podatkovnih datoteka
- 87 multimedijskih datoteka
    - 69 fotografija
    - 9 video zapisa

Pronađene podatkovne datoteke predstavljaju skup datoteka koje su nekategorizirane od strane alata. Slika ispod prikazuje dohvaćene nekategorizirane datoteke gdje je vidljivo kako su prve dvije datoteke označene crvenim simbolom X, a to je identifikator koji simbolizira opravljenu izbrisanu datoteku. Daljnjim pregledom moguće je vidjeti i putanje direktorija, kao i veličine datoteke, datum i vrijeme nastanka, modificiranja i brisanja datoteke.



#	Name	Path	Size (byte	Created	Modified
1	.VR_dji_kbufTN	Image0 /MISC/IDX/.VR_dji_kbufTN	44	15.1.2021. 12:18:24(UTC+0)	15.1.2021. 12:18:24(UT
2	.VR_dji_oMjXP9	NO NAME/MISC/IDX/.VR_dji_oMjXP9	35	15.1.2021. 12:12:26	15.1.2021. 12:12:26
3	dji.gis	NO NAME/MISC/GIS/dji.gis	431568...	15.1.2021. 12:22:08	15.1.2021. 12:22:08
4	dji.gis	Image0 /MISC/GIS/dji.gis	431568...	15.1.2021. 12:21:58(UTC+0)	15.1.2021. 12:21:58(UT
5	DJI_0041.SRT	NO NAME/DCIM/100MEDIA/DJI_0041.SRT	879311	15.1.2021. 11:56:50	15.1.2021. 11:56:50
6	DJI_0042.SRT	NO NAME/DCIM/100MEDIA/DJI_0042.SRT	1015738	15.1.2021. 11:59:56	15.1.2021. 11:59:56
7	DJI_0053.SRT	NO NAME/DCIM/100MEDIA/DJI_0053.SRT	883983	15.1.2021. 12:04:20	15.1.2021. 12:04:20
8	DJI_0074.SRT	NO NAME/DCIM/100MEDIA/DJI_0074.SRT	507406	15.1.2021. 12:10:22	15.1.2021. 12:10:22
9	DJI_0075.SRT	NO NAME/DCIM/100MEDIA/DJI_0075.SRT	126474	15.1.2021. 12:12:18	15.1.2021. 12:12:18
10	DJI_0076.SRT	NO NAME/DCIM/100MEDIA/DJI_0076.SRT	112672	15.1.2021. 12:12:44	15.1.2021. 12:12:44
11	DJI_0107.SRT	Image0 /DCIM/100MEDIA/DJI_0107.SRT	2370256	15.1.2021. 11:43:18(UTC+0)	15.1.2021. 11:43:18(UT
12	DJI_0119.SRT	Image0 /DCIM/100MEDIA/DJI_0119.SRT	374245	15.1.2021. 11:46:22(UTC+0)	15.1.2021. 11:46:22(UT
13	DJI_0124.SRT	Image0 /DCIM/100MEDIA/DJI_0124.SRT	790661	15.1.2021. 12:20:30(UTC+0)	15.1.2021. 12:20:30(UT
14	IndexerVolumeGuid	NO NAME/System Volume Information/Ind...	76	18.1.2021. 9:48:56	18.1.2021. 9:48:58
15	IndexerVolumeGuid	Image0 /System Volume Information/Index...	76	18.1.2021. 8:48:57(UTC+0)	18.1.2021. 8:48:58(UTC

Slika 18. Dohvaćene nekategorizirane datoteke zrakoplova DJI Mavic Air

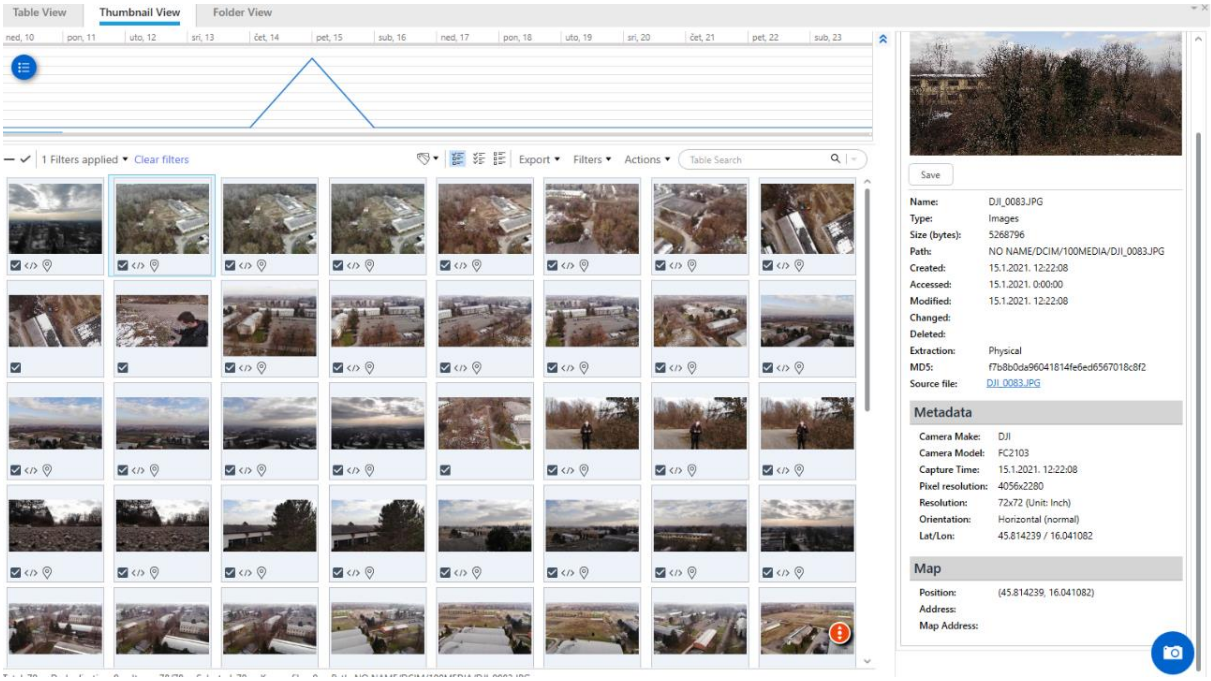
Za prvu datoteku naziva .VR_dji_kbufTN nije moguće točno odrediti o kakvoj je datoteci riječ. No prema putanji Image0/MISC/IDX/.VR_dji_kbufTN može se jedino pretpostaviti kako je ova datoteka zapravo fotografija, iako je uobičajena putanja fotografija pohranjenih na unutarnjoj i vanjskoj memoriji DCIM/100MEDIA. Vrijeme nastanka navedene datoteke je isto kao i kada je datoteka posljednji put modificirana i kada je posljednji put pristupljeno njoj. Vrijeme brisanja ove datoteke nije zabilježeno.

Druga datoteka, .VR_dji_oMjXP9 s putanjom NO NAME/MISC /IDX/.VR_dji_oMjXP9 predstavlja nepoznanicu jer iz putanje datoteke, ali i samog imena nije moguće naslutiti o kakvoj datoteci je riječ. Ova datoteka kao i prethodna nema vrijeme brisanja, ali vrijeme nastanka, modificiranja i posljednjeg pristupa je isto. Preostale nekategorizirane datoteke su datoteke formata .GIS i .SRT.

U nastavku izvještaja vidljiva je tablica Locations koja se sastoji od 69 multimedijskih datoteka, točnije fotografija gdje su prikazani lokacijski podatci uz svaku fotografiju te vrijeme nastanka fotografije.

Od ukupno 87 multimedijskih datoteka, 9 videozapisa ne sadrži podatke o lokaciji nastanka videozapisa, ali vidljivi su naziv video zapisa u formatu .MP4 te je poznato vrijeme i datum nastanka video zapisa kao i putanja pohrane. Video zapise je moguće pregledati unutar sučelja alata Physical Analyzer.

Prilikom pregleda informacija o video zapisu moguće je dodatno pregledati osnovne informacije o videozapisu. Osim navedenog, moguće je pregledati videozapis u heksadecimalnom zapisu unutar istoimenog preglednika. Uz 9 videozapisa dohvaćeno je 9 datoteka formata .SRT koji su vezani uz svaki videozapis.



Slika 19. Analiza fotografija alatom Physical Analyzer

Dohvaćenih 69 fotografija nalazi se u .JPG formatu, te za svaku fotografiju poznata je lokacija nastanka, naziv, vrijeme i datum nastanka fotografije. Moguće je svaku fotografiju pregledati u izborniku alata, ali prema poznatim metapodatcima i pronaći na integriranoj mapi alata u izborniku Map. Kako su fotografije uistinu bogate metapodatcima, istima je moguće pristupiti otvaranjem kartice File info.

U odnosu na video zapise, moguće je saznati puno više informacija o svakoj fotografiji, prvotno datum i vrijeme nastanka fotografije, informacije o senzoru kamere, rezoluciju, kontrast, lokaciju, udaljenost od fotografiranog subjekta i pregršt ostalih informacija.

Xiaomi Redmi Note 4X

Nakon napredne logičke ekstrakcije podataka mobilnog uređaja, provedena je analiza ekstrahiranih podataka. Iako su interes ekstrakcije i analize mobilnog uređaja podatci nastali između mobilnog uređaja i bespilotnog zrakoplova, pronađeni su drugi razni podatci koji mogu biti od pomoći pri samom slučaju. Bitno je znati kako prilikom provođenja sudskog procesa forenzički istražitelji ne smiju tražiti, ekstrahirati niti analizirati podatke koji nisu interes istrage. Ukoliko učine suprotno, svi pronađeni dokazi mogu biti odbačeni i istraga se mora ponavljati.

Analizom je ustanovljeno kako logičkom ekstrakcijom nisu oporavljeni podatci memorijske kartice koja je prethodno formatirana, čime je dokazano da napredna logička ekstrakcija ne može oporaviti obrisane podatke. Kao i kod izvještaja analize bespilotnog zrakoplova, na samom početku nalaze se informacije vezane za mobilni uređaj, ekstrakciju i sažetak.

Ekstrakcijom je dohvaćeno sljedeće:

- 4 kontakta
- 98 podatkovnih datoteka
    - 1 arhivska datoteka
    - 3 audio datoteke
    - 78 slika
    - 7 tekstualnih datoteka
    - 9 videozapisa

Pretragom rezultata analize utvrđeno je kako tekstualni zapisi formata .TXT nisu vezani za letačku aplikaciju DJI GO 4, ali ni bespilotni zrakoplov, nego uz Xiaomi servis usluga mobilnog uređaja. Audio datoteke nisu bitne jer navedene pripadaju Google servisu. Podatci vezani za aplikaciju DJI GO 4 su fotografije i video zapisi. Uvidom u iste ustanovljeno je kako su dohvaćene fotografije formata .JPG, bez metapodataka kao i bez podataka o lokaciji nastale fotografije.

Riječ je o naslovnim fotografijama čija je kvaliteta smanjena i takva fotografija umanjuje svoju vrijednost kao dokazni materijal u odnosu na primjerice one fotografije dohvaćene iz bespilotnog zrakoplova. Pregledom videozapisa pronađenih na uređaju, ustanovljeno je kako kvaliteta videozapisa nije kao kod izvornog videozapisa, postoji prisutnost artefakta.

5.3.2. Analiza podataka alatom Oxygen Forensics Detective

DJI Mavic Air

Prije početke analize podataka, učitana je *dump* datoteka fizičke ekstrakcije nastale na UFED Touch 2 uređaju jer, kako je prethodno rečeno, Oxygen Forensics Detective nema podršku za ekstrakciju podataka s DJI Mavic Air zrakoplova. Učitavanje *dump* datoteke napredne logičke ekstrakcije nije bilo moguće, stoga je učitana samo fizička ekstrakcija. Netom prije učitavanja viđene su prednosti i mogućnosti koje nudi ovaj alat, kao što su:

- Provjera *hash* vrijednosti
- Oporavci izbrisanih datoteka
- Odabir backup-a
- Odabir datoteka koje nisu od interesa
- Napredna analiza (prepoznavanje lica, kategorizacija fotografija)

Nakon 52 minuta dobiveni su rezultati unesene *dump* datoteke fizičke ekstrakcije i tu je započela analiza ekstrahiranih podataka s bespilotnog zrakoplova, a pritom je stvoren i izvještaj. Izvještaj ove ekstrakcije sastoji se od 8 datoteka .PDF formata, a u svakoj datoteci opisano je ono što je pronađeno i prikazano na jasan i razumljiv način. Navedene su informacije o uređaju kao i datotekama pronađenih na uređaju, ključni dokazi, rezultati zadane pretrage, statistika, vremenska crta i OCR (engl. *Optical Character Recognition*).U sažetku rezultata prikazanom na početku izvještaja, automatiziranim analitičkim pregledom alat je na fotografijama prepoznao i upozorio na jedan pronađeni ključni dokaz, oružje. Iako je je automatizirana analitika poželjna i ona ubrzava analizu ekstrahiranih podataka, treba biti oprezan i samostalno pregledati podatke jer postoji opasnost od pogreške kao tijekom analize u radu. Ključni dokaz kojega je alat prepoznao kao oružje je kontroler bespilotnog zrakoplova korišten prilikom upravljanja zrakoplovom (slika 20).



Slika 20. Lažno pozitivan ključni dokaz

Funkcija prepoznavanja lica na fotografijama nastalih korištenjem bespilotnog zrakoplova nije potpuno ispravna, odnosno razni drugi predmeti su prepoznati kao lice. Uz funkciju prepoznavanja lica, alat ima mogućnost prepoznavanja spola, rase, godina kao i dodataka koje osoba nosi. Automatizirano rješenje koje pruža ovaj alat nije u potpunosti razvijeno i potrebno je daljnje poboljšanje ove mogućnosti.

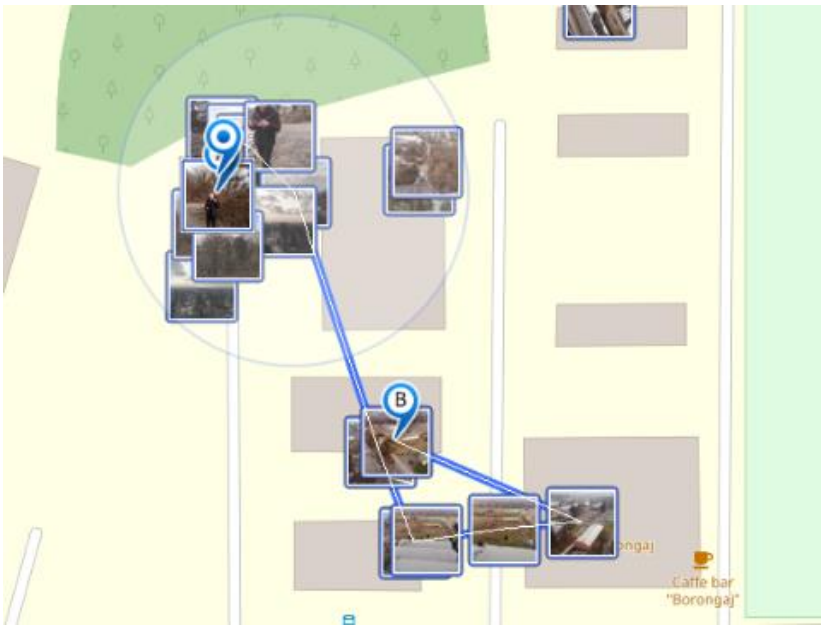
Ukupno je dohvaćeno 233 datoteka, od toga je 131 obrisana datoteka s unutarnje pohrane bespilotnog zrakoplova. Oxygen Forensics Detective nudi odličan prikaz datotečnog stabla i na jasan način prikazuje gdje se nalaze dohvaćene datoteke kao i njihov broj. Physical Analyzer pak ne nudi informacije o lokaciji pohrane datoteka. Tako je na internoj pohrani pronađeno 66 datoteka, a na memorijskoj kartici 36.

Dvije izbrisane datoteke koje su prethodno dohvaćene ekstrakcijom UFED Touch 2, analizirane su pomoću Oxygen Forensics Detective te je utvrđeno kako je VR_dji_kbufTN pohranjen na memorijskoj kartici, a datoteka .VR_dji_oMjXP na memoriji zrakoplova. Za iste nije moguće saznati o kakvim je vrstama datoteke riječ.

Preostali broj datoteka oporavljenih s memorijske kartice čini 68 fotografija .JPG formata, od kojih je veliki dio kompromitiran i nije moguće vidjeti sadržaj fotografije. Fotografije čiji je sadržaj vidljiv su umanjene, odnosno riječ je o naslovnim fotografijama (engl. *thumbnail*). Osim fotografija oporavljen je veliki broj audio zapisa, točnije njih 44, ali reprodukcija istih nije bila moguća. Uz oporavljenih 16 izbrisanih video zapisa, oporavljene su 3 tekstualne datoteke formata .UTF8. Datum brisanja datoteka nije zabilježen.

Bitno je napomenuti kako Physical Analyzer prilikom analize obiju ekstrakcija nije uspio oporaviti izbrisane datoteke kao što je to postignuto upotrebom Oxygen Forensics Detective. Analizom podataka pohranjenih na memorijskoj kartici bespilotnog zrakoplova pronađene su razne datoteke, prvenstveno veliki broj multimedijskih datoteka.

Sve fotografije nastale kamerom letjelice i pohranjene na memorijskoj kartici su dohvaćene i sadrže veliki set metapodataka. Identičan način prikaza EXIF podataka posjeduje i Physical Analyzer. Daljnjom analizom metapodataka, pronađene su koordinate lokacije nastanka svake fotografije. Korištenjem dodatka Maps unutar alata Oxygen Forensics Detective, moguće je sve fotografije s poznatim lokacijskim podatcima prikazati na karti, rekonstruirati redoslijed fotografiranja kao i rutu leta. Ruta leta tijekom koje su nastale fotografije prikazana je u realnom vremenu sa svim pripadajućim oznakama, vidljivo na slici 21.



Slika 21. Ruta leta tijekom nastanka fotografija

Prilikom pregleda svih datoteka, moguće je vidjeti točnu putanju direktorija gdje je navedena datoteka pohranjena. Pronađena 3 videozapisa moguće je pogledati unutar samog alata, ali i malu količinu metapoadataka videozapisa. Kao i u prethodnoj ekstrakciji uz video zapise pronađene su .SRT datoteke kao i naslovne fotografije. Uz iste dohvaćena je GIS datoteka koja, kao i u slučaju analize Physical Analyzer, nije kategorizirana kao GIS datoteke, te sistemska datoteka IndexerVolumeGuid koja je vezana uz informacije o pohrani.

Analizom podataka pronađenih na unutarnjoj memoriji uređaja utvrđeno je kako nije primijećena niti jedna anomalija jer je korištena ista metoda ekstrakcije kao i analize, sukladno tome ne postoji odstupanje. Sadržaj datoteka na unutarnjoj pohrani identičan je sadržaju na memorijskoj kartici, samo je u pitanju veća količina podataka pronađenih na unutarnjoj pohrani.

Rezultat veće količine podataka, odnosno datoteka pohranjenih na unutarnjoj memorije je što su postavke pohrane multimedijskih datoteka većinu vremena leta bile postavljene za spremanje u unutarnju pohranu zrakoplova.

U unutarnjoj pohrani zrakoplova pronađeno je:

- 45 fotografija
- 6 videozapisa
- 6 .SRT datoteka
- 6 naslovnih fotografija
- 1 GIS datoteka
- 1 sistemska datoteka (IndexerVolumeGuid)

Xiaomi Redmi Note 4X

Provođenje fizičke ekstrakcije podataka mobilnog uređaja i memorijske kartice alatom Oxygen Forensics Detective trajalo je 52 minute. Završetkom ekstrakcije kreiran je izvještaj koji će biti od pomoći prilikom analize. Izvještaj istrage sastoji se od nekoliko dokumenata, kao i kod slučaja bespilotnog zrakoplova, gdje je svaka skupina podataka i informacija izdvojena u zaseban PDF ili Excel dokument.

Oxygen Forensics Detective je fizičkom ekstrakcijom mobilnog uređaja prvotno pronašao bitne podatke o vlasniku mobilnog uređaja; ime i prezime, email adresu Google servisa kao i detaljne podatke o mobilnom uređaju i SIM kartici. Iako prvotno ovi podatci nisu glavni cilj analize, oni mogu biti korisni jer je moguće saznati tko je vlasnik mobilnog uređaja.

Budući da je mobilni uređaj prethodno vraćen na tvorničke postavke i *root-an,* oporavljen je veliki broj izbrisanih podataka. Ukupno je opravljeno 38 kontakata iz memorije mobilnog uređaja, ali bilo kakva komunikacija SMS ili email-om od prije nije pronađena. Podatci koji mogu biti od koristi prilikom provođenja istraživanja slučaja gdje je mobilni uređaj dokazni materijal su identifikacijski podatci korisnika uređaja, poput korisničkih imena za razne aplikacije, email, ali i bilješke o povezivanju na WiFi pristupnu točku. Tijekom istrage je otkriveno kako je uređaj bio spojen samo na jednu pristupnu točku, poznat je naziv, ali i lozinka te pristupne točke.

Ekstrakcijom memorijske karticom uspješno je oporavljen veliki broj datoteka koji se nalazi na njoj, točnije 37044 datoteke. Daljnjim pregledom sadržaja memorijske kartice utvrđeno je kako niti jedna multimedijska datoteka, ali ni ostale vrste datoteka nisu produkt korištenja bespilotnog zrakoplova niti letačke aplikacije DJI GO 4. Ovom metodom pronađene su naslovne fotografije snimljenih videozapisa koje ne sadržavaju metapodatke. Naprednom logičkom ekstrakcijom pomoću UFED Touch 2 nisu pronađene fotografije, ali ni glazba i video zapisi koje se pohranjuju na uređaj ukoliko je instalirana aplikacija DJI GO 4.

Oxygen Forensics Detective je prethodno navedene datoteke ekstrahirao i moguće je provesti uvid u iste datoteke. Automatsko pretraživanje ključnih dokaza sa fotografije je podržano na naslovnim, ali i na oporavljenim fotografijama s memorijske kartice. Navedenim pretraživanjem ustanovljeno je kako postoji sadržaj od interesa za stručnjake jer se na nekim fotografijama nalazi oružje, alkohol i nedozvoljene supstance. I dalje je na nekim fotografijama lažno prepoznat dokaz.

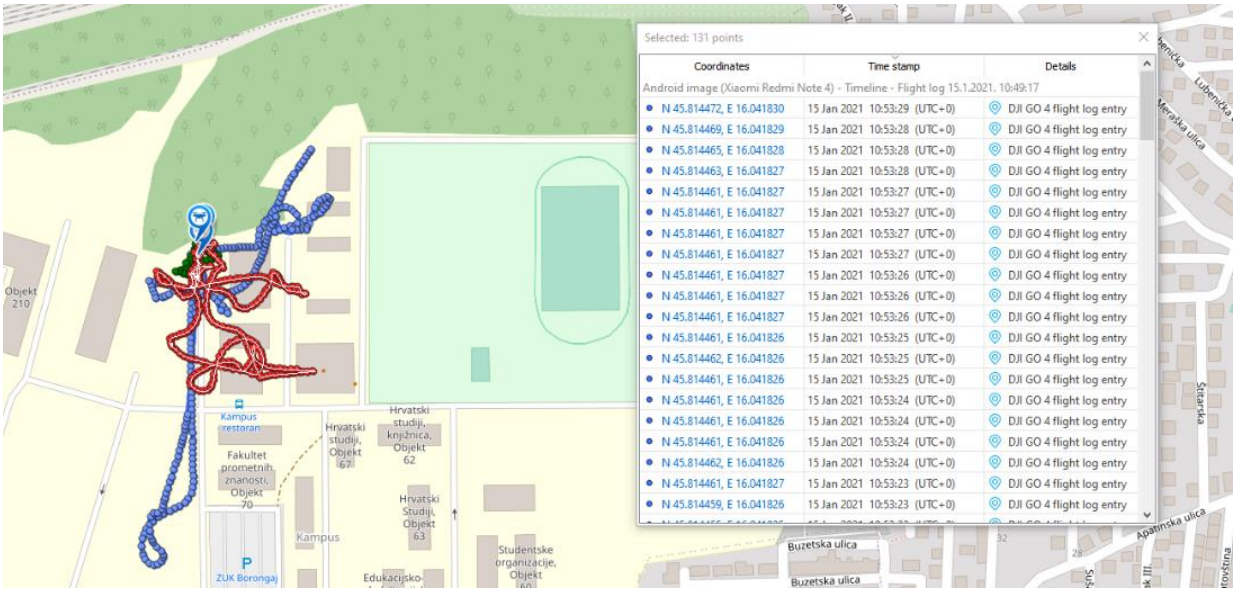
Budući da Oxygen Forensics Detective podržava duboku analizu svake aplikacije koja se nalazi na mobilnom uređaju, tako je moguće analizirati sadržaj DJI GO 4 aplikacije. Analizom je automatski kreiran izvještaj ekstrakcije aplikacije DJI GO 4 koji se sastoji od 3087 stranica. U samom izvještaju detaljno su navedeni svi video zapisi te podatci o njima, bez metapodataka. Iz izvještaja je vidljivo i tko je vlasnik letjelice.

Ono što je bitno i čini veliku razliku u odnosu na ekstrakciju i analizu podataka pomoću UFED Touch 2 i Physical Analyzer jesu dobiveni zapisi aplikacije DJI GO 4 o letu. Letačke aktivnosti koje su izvršene 15. siječnja detaljno su prikazane u izvještaju, gdje je svaki let prikazan zasebno. Zapisi o letu (engl. *Flight log*) svakog leta sastoji se od početne točke kao i završne točka leta. Svaka točka leta sastoji se od:

- Koordinata
- Vremenske oznake
- Vremena leta u toj točki
- Visine
- Brzine (prema X,Y i Z osi)

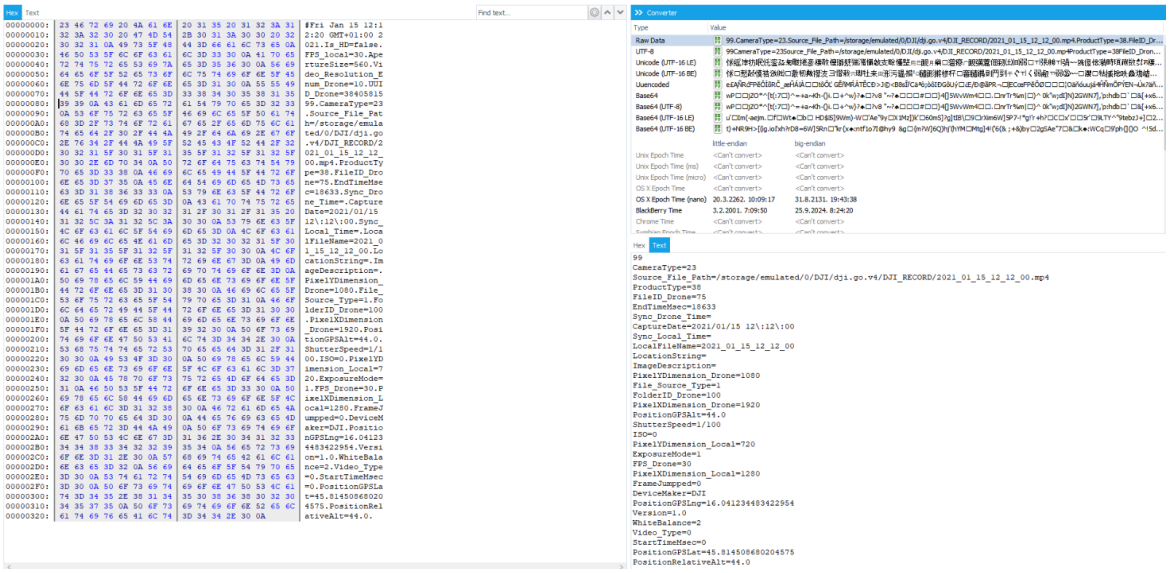
Ovakav uvid u letačke aktivnosti može biti od velike pomoći jer forenzički istražitelji mogu zahvaljujući velikom broju točaka rekonstruirati gdje je sve letio bespilotni zrakoplov te brzinu kojom je letio. Uz poznatu brzinu moguće je odrediti je li letjelica u danom trenutku i danoj lokaciji mirovala ili je letjela.

Unutar alata Oxygen Forensics Detective, pomoću zapisa o letu moguće je vizualizirati na mapi sve rute leta zrakoplova. Grafički je prikazana brzina, ali i visina za svaki let zasebno, (slika 22). Uz to prikazana je i duljina leta kao i vrijeme trajanja leta.



Slika 22. Prikaz rute lete i koordinata pomoću alata Oxygen Forensics Detective

Dokazi koji su dohvaćeni ovom metodom su i log zapisi gdje je daljnjim pregledom ustanovljeno kako je riječ o metapodatcima o fotografijama, (slika 23).



Slika 23. Metapodatci fotografije

5.3.3. Analiza ručne ekstrakcije

Tijekom rada u laboratoriju, nakon učinjenih ekstrakcija podataka alatima, izvršena je i ručna ekstrakcija podataka bespilotnog zrakoplova, ali i mobilnog uređaja. Ručna ekstrakcija predstavlja najjednostavniju metodu ekstrakcije, odnosno dohvaćanje podataka prijenosom istih s uređaja na medij za pohranu ili forenzičku radnu stanicu. Provođenjem iste može doći do izmjene podataka.

DJI Mavic Air

Ručnom ekstrakcijom podataka unutarnje pohrane bespilotne letjelice i memorijske kartice pronađene su fotografije, videozapisi i datoteke .SRT formata. Datoteke .SRT formata prethodno su spominjane i prilikom fizičke ekstrakcije, jedna od datoteka je otvorena pomoću programa za pisanje teksta, Notepad.

Otvaranjem ove datoteke otkriveni su metapodatci svakog videozapisa u jednom okviru slike. Za svaki okvir slike zabilježeni su podatci o kameri (ISO, Shutter, Fnum,Color_md) vrijeme snimanja i redni broj okvira. Pokretanjem videozapisa programom VLC, moguće je vidjeti unutar video podatke .SRT datoteka, (slika 24).



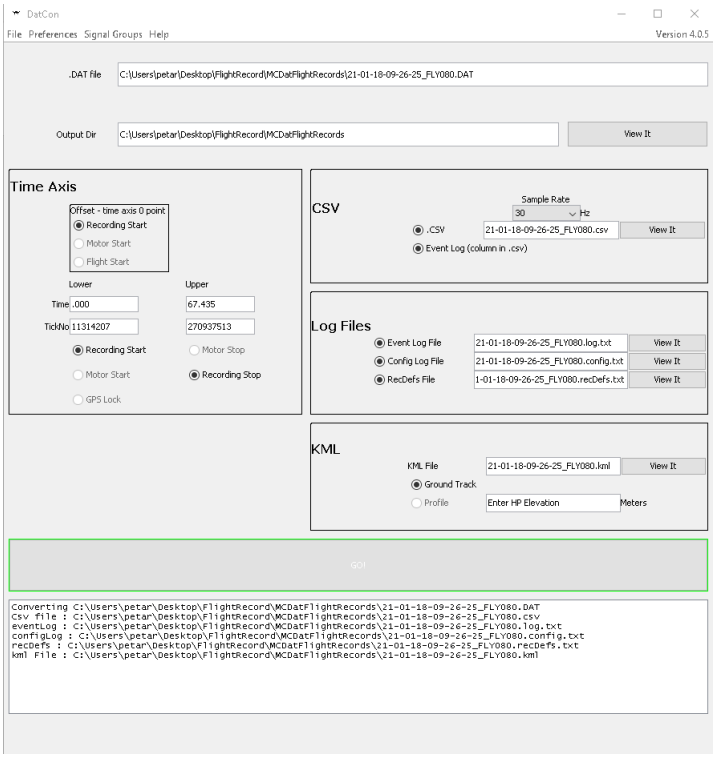
Slika 24. Prikaz .SRT datoteke u okviru videozapisa

Na forenzičkoj radoj stanici unutar operativnog sustava Windows pregledom svojstva fotografije moguće je saznati metapodatke o fotografijama bez korištenja forenzičkih alata. Metapodatci poznati iz svake fotografije su vrijeme nastanaka fotografije, postavke kamere i GPS podatci. Ručnom pretragom moguće je doći i do datoteka formata .THM, odnosno naslovnih fotografija, a daljnjim pregledom moguće je pronaći i datoteku .GIS formata.

Xiaomi Redmi Note 4X

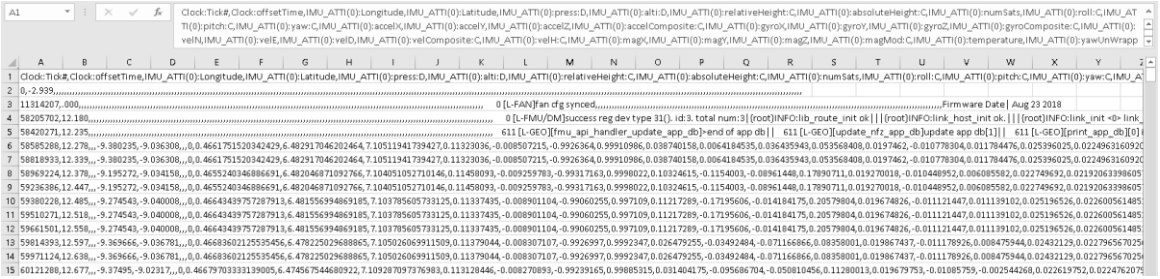
Analizom uređaja Xiaomi Redmi Note 4X mogu se pregledati podatci koji su korisni u forenzičkoj istrazi. Provođenjem ručne ekstrakcije ekstrahiran je sadržaj koji se nalazi na mobilnom uređaju. Pregledom je ustanovljeno kako postoje dvije DJI mape, jedna na mobilnom uređaju, a druga na memorijskoj kartici uređaja koja je prazna. Daljnjim pregledom mape DJI.GO.V4 pronađena je mapa s naslovnim fotografijama kao i mapa s video sadržajem. Fizičkom ekstrakcijom podataka mobilnog uređaja pronađene su fotografije i videozapisi s uputama za let, a iste slike i videozapisi uspješno su ekstrahirani ovom ekstrakcijom.

U mapi DJI nalazi se veliki broj log zapisa. Neke log zapise nije bilo moguće interpretirati, poput velikog broja log zapisa *cache* memorije letjelice koji uključuju zapise o navigaciji, kontroleru i ažuriranjima *firmwera*. Osim vidljivih log zapisa, datoteke formata .DAT u mapi FlightRecorder sadrže izuzetno bitne informacije o letačkim aktivnostima. Budući da je riječ o .DAT datoteci, istu nije moguće otvoriti programima koje ima svaki prosječni korisnik na računalu, nego je potrebno koristiti poseban softver koji će interpretirati podatke. Softver koji je razvijen za potrebe interpretacije i pretvorbe datoteka zapisa leta je DatCon. O DatCon-u je bilo riječi u poglavlju 3.



Slika 25. Sučelje programa DatCon

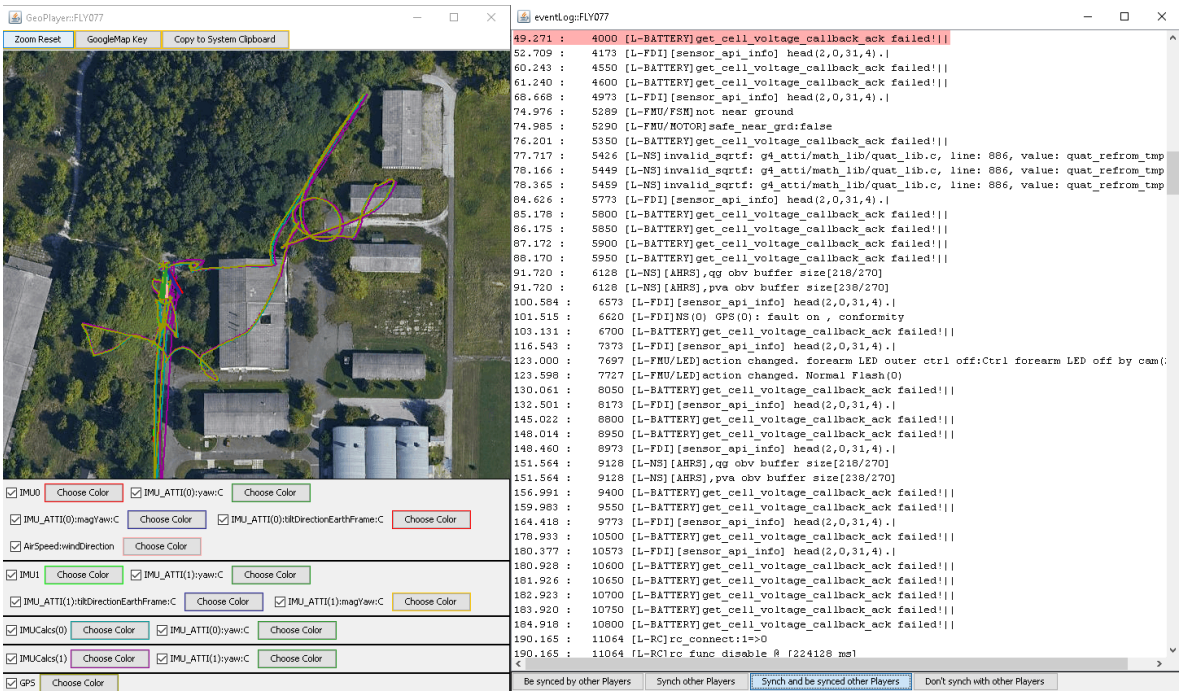
Učitavanjem .DAT datoteke u softver DatCon, ista datoteka je pretvorena u Excel datoteku.



Slika 26. Prikaz podataka nastalih pretvorbom .DAT datoteke

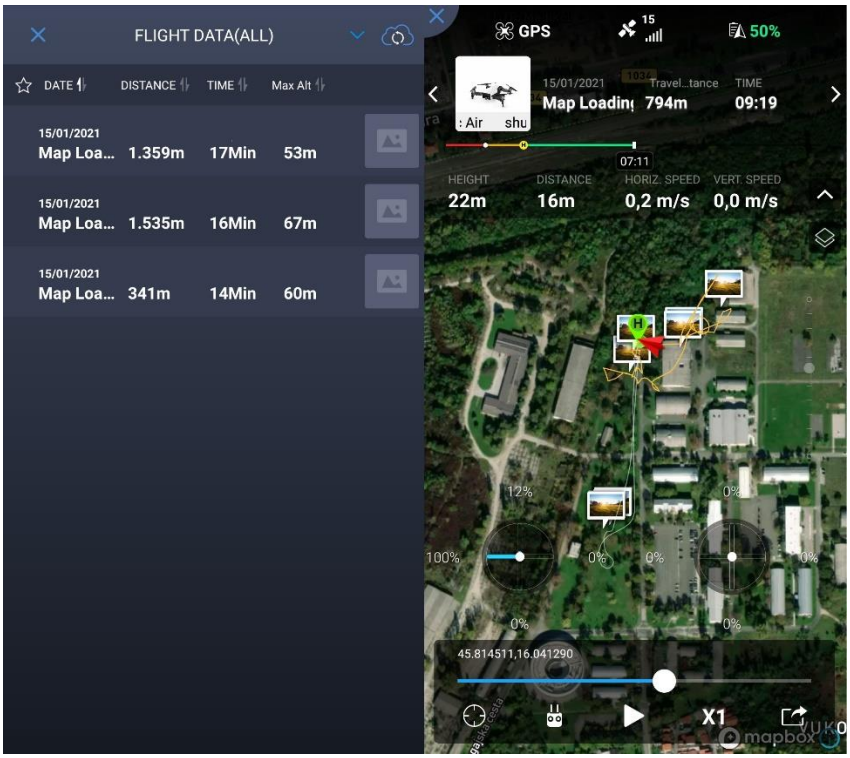
Zapisi leta prikazani su u Excel tablici i tablice sadrže veliki broj podataka, ali je pregled istih izuzetno nezgodan i nepraktičan (slika 26). Neki od navedenih podataka su: vrijeme polijetanja, visina, lokacija, napon i stanje baterije, brzina letjelice, stanje motora, smjer i brzina vjetra i sl.

Kako bi vizualizirali letačke aktivnosti bespilotnog zrakoplova, korišten je program CsvView. Kako bi prikazali putanju letačkih aktivnosti, potrebno je u program CsvView učitati .CSV datoteku nastalu pretvorbom .DAT datoteke programom DatCon.



Slika 27. Prikaz rute leta i log zapisa

Osim putanje letačkih aktivnosti, prikazan je log zapis koji je zabilježen tijekom navedenih aktivnosti kao i podatci o zrakoplovu. Ovim log zapisom prikazan je veliki broj događaja zabilježenih tijekom leta, ali interpretacija ovog zapisa nije jednostavna i zahtijeva dobro znanje o ovoj materiji (slika 27).



Slika 28. Prikaz zapisa leta unutar aplikacije DJI GO 4

Letačka aplikacija na mobilnom uređaju također može biti od pomoći prilikom forenzičke istrage. Detaljnim pregledom aplikacije primijećeno je kako i aplikacija nudi detaljan uvid u prethodne letačke aktivnosti.

U aplikaciji je moguće vidjeti svaki let odvojeno te je putanja leta vizualizirana na karti, gdje su posebno naznačene lokacije snimljenih fotografija. Nadalje, prikazani su podatci poput stanja baterije, broja navigacijskih satelita, vrijeme leta, visine, brzine vjetra i brzine zrakoplova (slika 28).

Naposljetku, moguće je i prikazati simulacije upravljačkih komandi kontrolera, odnosno vidljiv je položaj upravljačkih palica tijekom leta.

5.4. Usporedba alata

U nastavku, radi boljeg uvida i razumijevanja rezultata ostvarenih istraživanjem u ovome radu pomoću tablice 5. prikazane su neke od mogućnosti korištenih forenzičkih alata UFED Touch 2, UFED Physical Analyzer te Oxygen Forensics Detective.

Tablica 5. Mogućnosti forenzičkih alata korištenih u radu

Alat	UFED Touch 2, UFED Physical Analyzer		Oxygen Forensics Detective
Uređaj	DJI Mavic Air		
Ekstrakcija	Datotečnog sustava	Fizička	Nije podržana
Trajanje ekstrakcije (min)	20	54	
Broj datoteka	**123**	**102**	**233**
Informacije o uređaju	DA	DA	DA
Prikaz datotečnog stabla	NE	NE	DA
Baza podataka	DA	DA	NE
Snimljene fotografije	NE	DA	DA
Videozapisi	NE	DA	DA
Lokacija fotografija	NE	DA	DA
Metapodatci	NE	DA	DA
Vremenska crta događaja	NE	DA	DA
Log zapisi	DA	DA	DA
Ruta leta	NE	NE	NE
Oporavak obrisanih podataka	NE	DA	DA[4]
Napredna analitika	NE	NE	DA
Napredna pretraga	NE	NE	DA

[4] Oporavak podataka memorijske kartice

Uređaj	Kontroler	
Ekstrakcija	Nije podržana	
Uređaj	Xiaomi Redmi Note 4X	
Ekstrakcija	Napredna datotečna	Fizička
Trajanje ekstrakcije (min)	5	52
Količina datoteka	99	59615 (37044)[5]
Informacije uređaju	DA	DA
Prikaz datotečnog stabla	NE	DA
Baza podataka	NE	DA
Imenik	DA	DA[6]
SSID	NE	DA
E-mail poruke	NE	DA
Korisnički računi	NE	DA
Naslovne fotografije	DA	DA
Snimljene fotografije	NE	NE
Videozapisi	DA	DA
Lokacija fotografija	NE	DA
Metapodatci	DA	DA
Vremenska crta događaja	NE	DA
Log zapisi	DA	DA
Ruta leta	NE	DA
Oporavak obrisanih podataka uređaja i memorijske kartice	NE	DA
Napredna analitika	NE	DA
Napredna pretraga	NE	DA
Aplikacija DJI GO 4	NE	DA
Potvrda integriteta podataka		
MD-5	DA	DA
SHA-1	DA	DA
SHA-256	DA	DA
SHA3-256	NE	DA
PhotoDNA	NE	DA
Formati izvještaja		
CSV	DA	NE
HMTL	DA	DA
PDF	DA	DA
TXT	NE	NE
XML	DA	DA

[5] Broj oporavljenih podataka memorijske kartice
[6] Uključujući izbrisane kontakte

Iz tablice je jasno vidljivo kako je Oxygen Forensics Detective, iako ne podržava ekstrakciju podataka bespilotnog zrakoplova DJI Mavic Air, dohvatio puno više podataka iz *image* zrakoplova, nego li je to postignuto UFED Physical Analyzer-om. Ekstrakcijom datotečnog sustava koristeći UFED Touch 2 i Physical Analyzer nisu dohvaćeni bitni dokazi, poput fotografija i video zapisa nastalih kamerom zrakoplova, ali ono što je dohvaćeno i može biti korisno u istrazi su log zapisi aktivnosti senzora. Fizičkom ekstrakcijom zrakoplova uspješno su dohvaćene fotografije, ali i videozapisi te metapodatci, uključujući one o fotografijama i videozapisima. Ono što nije ostvareno provođenjem datotečne ekstrakcije, a uspjelo je prilikom fizičke ekstrakcije, oporavak je izbrisanih datoteka s unutarnje pohrane zrakoplova. Provođenjem analize alatom Oxygen Forensics Detective moguće je oporaviti i izbrisane datoteke memorijske kartice zrakoplova, iako je u našem slučaju jedan dio datoteka kompromitiran. Nadalje, bitno je naglasiti kako Oxygen Forensics Detective posjeduje mogućnost napredne analitike multimedijskih datoteka, tj. detekciju lica, neprimjerenog sadržaja (pornografija, droga i alkohol), ali i oružje. Prilikom analize, detektirano je nekoliko lažno pozitivnih dokaza.

Ekstrakcija podataka mobilnog uređaja Xiaomi Redmi Note 4X podržana je od strane jednog i drugog alata, samo što UFED Touch 2 omogućava manje složenu ekstrakciju, naprednu datotečnu ekstrakciju. Ovom metodom s mobilnog uređaja, ali i memorijske kartice nisu oporavljene izbrisane datoteke. Osim navedenih datoteka, nisu ekstrahirani trenutni podatci (E-mail poruke, korisnički računi, SSID, itd.). Budući da je na uređaju za potrebe leta instalirana letačka aplikacija DJI GO 4, ista je generirala podatke vezane uz bespilotni zrakoplov, odnosno letačke aktivnosti i multimedijski sadržaj. Snimljene fotografije nisu dohvaćene, ali jesu naslovne fotografije i videozapisi, s određenim setom metapodataka.

Alatom Oxygen Forensics Detective provedena je fizička ekstrakcija podataka mobilnog uređaja. Fizičkom ekstrakcijom ekstrahirana je velika količina značajnih i obrisanih podataka. Ekstrahirani su obrisani kontakti imenika, e-mail poruke, kao i velika količina obrisanih podataka memorijske kartice. Kako Oxygen Forensics Detective posjeduje mogućnost analize svake aplikacije koja se nalazi na mobilnom uređaju, tako je provedena analiza letačke aplikacije DJI GO 4. Analizom aplikacije, prikazana su sva 3 leta, uz sve parametre koji ih opisuju (vrijeme leta, visina i brzina) uz poznate koordinate lokacije u svakom trenutku leta kao i vizualizaciju rute leta na karti. Osim navedenog, na kraju analize kreiran je detaljan izvještaj analize aplikacije DJI GO 4 od 3087 stranica, koji može biti izuzetno koristan u sudskom procesu. Važno je naglasiti kako Oxygen Forensics Detective podržava veliki broj *hash* algoritama za potrebe provjere integriteta podataka. Analizom i sumiranjem svih podataka ekstrahiranih iz ova dva uređaja dolazi se do zaključka da je alat Oxygen Forensics Detective zadovoljavajući alat i da svojom analizom te ekstrakcijom podataka daje bolje rezultate u odnosu na alat UFED Touch 2. Ekstrakcija podataka kontrolera bespilotnog zrakoplova nije bila moguća.

6. Digitalna antiforenzika i protumjere zloupotrebe bespilotnih zrakoplova

Razvojem tehnologije uvijek se pojavljuje ona loša strana, mogućnost zloupotrebe. Zbog iznimno niske cijene i dostupnosti bespilotni zrakoplovi mogu u krivim rukama predstavljati veliki sigurnosni rizik, jer primjerice, moguće je modificirati bespilotni zrakoplov kako bi nosili ubojita sredstva i tako izvršili teroristički napad. Osim ekstremnih slučajeva zloupotrebe bespilotnog zrakoplova poput terorističkih aktivnosti, zrakoplov je moguće koristiti primjerice u svrhe organiziranog kriminala, ali i u konačnici narušavanje zabranjenih zona letenja i privatnosti.

U ovome poglavlju bit će opisane protumjere kojima je moguće spriječiti bilo kakvu nedozvoljenu aktivnost, ali i metode koje se koriste za prikrivanje digitalnih dokaza sustava bespilotnih zrakoplova.

6.1. Digitalna antiforenzika

Zbog mogućnosti kaznenog progona operatera u slučaju istrage zloupotrebe zrakoplova pribjegava se raznim metodama sakrivanja digitalnih tragova korištenja uređaja i tako se otežava istraga. Digitalna antiforenzika predstavlja alate i metode kojima se sprječava, ali i otežava proces forenzičke istrage.

6.1.1. Primjena digitalne antiforenzike na mobilni uređaj

Kako je mobilni uređaj dio sustava bespilotnog zrakoplova i sadrži digitalne dokaze, moguće je izvršiti proces antiforenzike kako bi spriječili pronalazak digitalnih dokaza. Samo neke od raznih metoda antiforenzike opisane su u nastavku teksta.

Sudden Death predstavlja najjednostavniji antiforenzički pristup. Aplikacija je prethodno instalirana na mobilni uređaj i konfigurirana tako da se automatski pokrene nakon svakog uključivanja uređaja. Posebnost ove metode jest da mobilni uređaj može detektirati, tj. prepoznati da je mobilni uređaj spojen na forenzičku radnu stanicu, odnosno alat. Ukoliko mobilni uređaj detektira da je povezan na forenzički alat, mobilni uređaj se isključuje, a svi podatci koji se nalaze na njemu se brišu, [49].

Skrivanje podataka predstavlja proces kojim se otežava pronalaženje podataka forenzičkim istražiteljima. Isti ti podaci ostaju na uređaju i dostupni su za upotrebu. Metode skrivanja podataka su steganografija, enkripcija i druge metode. Ukoliko se za skrivanje podataka koristi više metoda, moguće je u cijelosti spriječiti pronalazak podataka.

Brisanje povjerljivih podataka je još jedna od metoda antiforenzike koja kao i *sudden death* radi prema načelu detekcije povezivanja na forenzičku radnu stanicu, samo što se u ovome slučaju briše povjerljivi sadržaj. Korisnik uređaja može odabrati koji sadržaj je povjerljiv, te će isti biti obrisan ukoliko dođe do povezivanja uređaja na forenzičku radnu stanicu ili bilo koji forenzički alat.

Izmjena podataka na način da postanu nečitljivi osobama bez znanja o kriptografiji naziva se enkripcija. Ovo je jedna o najčešćih metoda antiforenzike, gdje se može u potpunosti kriptirati memorijska pohrana i onemogućiti pristup istoj.

Steganografija obuhvaća proces prikivanja informacija, gdje se iste te informacije prenose unutar nekog drugog oblika podataka. Primjer ovakve metode je popunjavanje ostatka podatkovnog prostora multimedijskih datoteka tajnim informacijama, koje je teško pronaći i izdvojiti od izvornih, [50].

6.1.2. Primjena digitalne antiforenzike na bespilotni zrakoplov

Forenzički stručnjaci prilikom provođenja istrage ne smiju zanemariti niti integritet digitalnih dokaza bespilotnog zrakoplova, jer nad istima je moguće provesti mjere kako bi spriječili pronalazak bitnih dokaza. Neke od prethodno navedenih metoda antiforenzike moguće je upotrijebiti i na podatcima bespilotnog zrakoplova. Kako bespilotni zrakoplovi mogu obogatiti sadržaj fotografija lokacijskim podatcima, ali i zabilježiti lokacije letačkih aktivnosti ponekada postoji potreba za prikrivanje tih podataka. Primjerice, ukoliko se vrši ilegalni nadzor moguće je prikriti sudjelovanje u nadzoru blokirajući GPS signal zrakoplova.

Kako bi onemogućili lokacijske dokaze, otpajanje GPS prijemnika s matične ploče bespilotnog zrakoplova čini se najboljom opcijom. Ali, bespilotni zrakoplovi posjeduju mehanizam koji detektira da neka komponenta nije spojena i tako sprječava pokretanje električnih motora zrakoplova i time onemogućava bilo kakav let, [51].

Prema izvoru [52], istraživanjem je dokazano kako je moguće blokirati prijem GPS signala zrakoplova postavljanjem aluminijske folije na kućište zrakoplova gdje se nalazi GPS prijemnik. Daljnjim istraživanjem utvrđeno je kako nisu pohranjeni lokacijski podatci u opisu fotografije. Ovakvim postupkom neće biti zabilježene lokacije od kud je letjelica poletjela (engl. *Home point*) kao i gdje je sletjela. Blokiranjem GPS prijemnika operator ima mogućnost leta u zabranjenom području.

Bespilotni zrakoplovi nemaju mogućnost stalnog napajanja i tako vremenska oznaka koja se dodaje fotografiji nije ona stvarna, odnosno ne predstavlja stvarni datum kao ni vrijeme nastanka fotografije. Za potrebe dodavanje točne vremenske oznake bespilotni zrakoplov sinkronizira vremensku oznaku s vremenom koji je na mobilnom uređaju. Samim time moguće je manipulirati vremenskim oznakama nastalih podataka tako što se izmjeni vrijeme i datum na mobilnom uređaju ili vremenska zona.

Ukoliko je korišten mobilni uređaj za upravljanje zrakoplovom, ekstrakcijom podataka moguće je doznati lokaciju gdje se nalazio operator za vrijeme upravljanja zrakoplovom. Kako bi sakrili lokacijske dokaze, koristi se softver za lažiranje lokacije mobilnog uređaja koji je javno dostupan i besplatan na Google Trgovina Play.

6.2. Protumjere zloupotrebe bespilotnog zrakoplova

Dostupnost i niska cijena besplatnih zrakoplova, zadala je veliku muku privatnim tvrtkama, upravama zračnih luka, vojsci, policiji, državnim tijelima i ostalima, te su oni u potrazi su za mjerama kojima bi spriječili bilo kakve ilegalne aktivnosti koja uključuje upotrebu bespilotnih zrakoplova. Zbog toga je razvijena nova grana tehnologije, C-UAS (engl. *Counter UAS*). C-UAS predstavlja sustav mjere detekcije, presretanja ili rušenje bespilotnog zrakoplova. C-UAS mjere moguće je podijeliti u dvije kategorije, detekcija zrakoplova i zaustavljanje zrakoplova.

6.2.1. Detektiranje bespilotnog zrakoplova

Za potrebe detektiranja bespilotnog zrakoplova potrebno je koristiti opremu koja omogućava detekciju, klasifikaciju i praćenje. Stoga je moguće koristiti slijedeće, [53]:

- RF (engl. *Radio Frequency*) analizator - uređaj čija je namjena detekcija radio komunikacije između kontrolera i zrakoplova na male udaljenosti. Ovisno o uređaju, moguće je otkriti MAC adresu zrakoplova i kontrolera, pa čak i pomoću triangulacije odrediti položaj.
- Optički senzori (kamera) - video kamere visoke kvalitete, dodatkom softvera kamera može prepoznati bespilotni zrakoplov, ali i teret. Veliki nedostatak kamera je smanjena sposobnost i detekcija tijekom loših vremenskih uvjeta.
- Akustični senzor (mikrofon) - za potrebe detekcije, odnosno izračuna smjera iz kojega bespilotni zrakoplov dolazi koristi se akustični senzor ili nekoliko njih. Nedostatak ovakve detekcije je osjetljivost na glasnu okolinu, domet, ali i nemogućnost određivanja udaljenosti zrakoplova.

- Radar – koristi se za nadzor kopna i mora, sukladno tome radari se koriste i za detekciju bespilotnih zrakoplova, ali mala dimenzija bespilotnih zrakoplova predstavlja problem prilikom detekcije. Prednost radara je velika preciznost kao i domet uz mogućnost stalnog praćenja zrakoplova te neovisnost o vremenskim uvjetima. Mana je neraspoznavanje bespilotnog zrakoplova i ptice kao i interferencija. Mikro-doppler radar je FMCW (engl. *Frequency Modulated Continuous Wave*) radar i za razliku od drugih radara omogućava identifikaciju bespilotnog zrakoplova vrlo lako, a isto tako raspoznaje zrakoplov i pticu.



Slika 29. C-UAS radarski sustav detekcije, [54]

6.2.2. Zaustavljanje bespilotnog zrakoplova

Ukoliko je detektiran nepoznati bespilotni zrakoplov nad područjem koji strogo zabranjuje letačke aktivnosti ili iste predstavljaju opasnost, ovlaštene osobe (vojska, policija, sl.) imaju pravo zaustaviti letačke aktivnosti što može u krajnjem slučaju značiti uništenje zrakoplova.

Mehanizmi zaustavljanja bespilotnih zrakoplova još uvijek su u razvoju, a trenutno je u upotrebi nekoliko mehanizama, najčešći su, [55]:

- Ometanje - cilj ometanja je prekid komunikacije između operatora bespilotnog zrakoplova i zrakoplova na način da se odašilje isti signal veće snage. Nedostatak ovakvog zaustavljanja jest da nije moguće znati što će se dogoditi s bespilotnim zrakoplovom, hoće li sletjeti ili će pasti. Ometanjem je moguće zrakoplov vratiti na mjesto uzlijetanja ukoliko zrakoplov ima mogućnost povrataka na mjesto uzlijetanja u slučaju prekida komunikacije. Na takav način moguće je doći do operatora zrakoplova.

- Mreže za hvatanje - hvatanje bespilotnih zrakoplova ovakvom metodom zahtijeva ispaljivanje mreže sa zemlje ili s bespilotnog zrakoplova. Budući da mreža blokira rada propelera dolazi do pada zrakoplova i za te potrebe koristi se padobran kako bi na siguran način prizemljili zrakoplov. Ukoliko se bespilotni zrakoplov hvata drugim bespilotnim zrakoplovom, zrakoplov ima mogućnost transporta uhvaćenog zrakoplova do željene lokacije.
- Ptice - vojske i policija nekih država odabrale su za borbu protiv bespilotnih zrakoplova ptice. Ovakav način hvatanja i rušenja zrakoplova zahtijeva trening ptica od mlade dobi.
- Direktna energija - predstavlja invazivnu mjeru kojom se bespilotni zrakoplov zaustavlja rušenjem ispaljivanjem laserskog snopa, ali i možebitnim uništenjem prilikom pada ili zapaljenja zrakoplova. Zbog navedenog, ova metoda možda neće uvijek biti najbolji izbor, jer nije sigurno upotrebljavati ovakav mehanizam zaustavljanja ukoliko postoji opasnost od pada zrakoplova na ljude nakon ispaljivanja laserskog snopa. Osim navedene mjere zaustavljanja bespilotnog zrakoplova, moguće je koristiti i vatreno oružje, što podrazumijeva upotrebu standardne municije te projektila.
- *Geofencing* - stvaranje imaginarne ograde, odnosno granice na karti gdje se svaki pokušaj ulaska u ograđeni prostor detektira i netko biva obaviješten. Tako za slučaj bespilotnog zrakoplova, ukoliko operator želi ući u ograđeno područje, zrakoplov odbija let, odnosno ulazak u područje koje je geografski ograđeno.

7. Zaključak

Posljednjih godina vidljiv je napredak u području informacijsko-komunikacijske tehnologije koja uvelike olakšava život. Pojavom bespilotnih zrakoplova određene djelatnosti ostvarile su mnoge prednosti. Razvojem tehnologije uvijek se pojavljuju i one loše strane, odnosno dolazi do njezine zloupotrebe. Zbog svojih sposobnosti bespilotni zrakoplovi mogu uvelike biti korišteni za neovlašteno nadziranje, ali i za razne kriminalne i terorističke aktivnosti. Kontroler bespilotnog zrakoplova u krivim rukama predstavlja veliku opasnost za ljude, za njihovu privatnost, ali i živote. Zbog sve češćih zlonamjernih letačkih aktivnosti, kao i terorističkih napada, bespilotni zrakoplovi postaju interes policijskih, obavještajnih i vojnih službi. Upotrebom bespilotnih zrakoplova korisnici ostavljaju digitalne tragove i zbog toga se pojavila potreba za pronalaskom i analizom digitalnih dokaza što je dovelo do pojave digitalne forenzike. Veliki problem predstavlja nepostojanje standardne procedure prilikom provođenja forenzičke istrage bespilotnog zrakoplova jer je ova grana digitalne forenzike nova disciplina i još je u razvoju.

U ovome diplomskom radu prikazana je procedura forenzičke istrage sustava bespilotnog zrakoplova, kojega čine bespilotni zrakoplov DJI Mavic Air, kontroler zrakoplova i mobilni uređaj. Bespilotni zrakoplov DJI Mavic Air sadrži veliku količinu digitalnih dokaza kao i mobilni uređaj, ali potrebno je pronaći način kako doći do tih dokaza kao i najbolji alat. Uz UFED Touch 2 u praksi je testiran i Oxygen Forensics Detective. Iako Oxygen Forensics Detective ne podržava ekstrakciju podataka bespilotnog zrakoplova, podržava analizu *image* ekstrahiranog uređajem UFED Touch 2. Sučelja oba alata su intuitivna i jednostavna, a postupak ekstrakcije je razumljiv. Na količinu ekstrahiranih podataka utječe izbor alata kao i metoda ekstrakcije, što je najbolje prikazano prilikom ekstrakcije podataka mobilnog uređaja. Fizičkom akvizicijom podataka bespilotnog zrakoplova pomoću oba alata dohvaćeni su multimedijski podatci kao i metapodatci, a alatom Oxygen Forensics Detective oporavljen je set obrisanih podataka memorijske kartice. Letačka aplikacija generira veliku količinu podataka koja može biti od pomoći prilikom forenzičke istrage. Ekstrakcija datotečnog sustava mobilnog uređaja ne dohvaća veliki broj podataka, dok fizička ekstrakcija dohvaća veliki broj prisutnih i izbrisanih podataka s uređaja. Fizičkom ekstrakcijom podataka mobilnog uređaja alatom Oxygen Forensics Detective moguće je dohvatiti sve podatke letačke aplikacije, poput ruta leta, iste interpretirati i vizualizirati. Iz rezultata diplomskog rada moguće je zaključiti da alat Oxygen Forensics Detective predstavlja konkurenciju alatu UFED Touch 2, kako po količini ekstrahiranih podataka, tako i detaljnoj analizi.

Forenzička istraga sustava bespilotnih zrakoplova zahtijeva puno vremena, ali i znanja. Kako bi se postigli što bolji rezultati i provela bolja analiza, potrebno je koristiti široku paletu forenzičkih, ali i ne-forenzičkih alata kao i veliki broj metodologija.

Popis Literature

[1] Digital Photography School: Aerial Time Lapse Basics with DJI Mavic Pro 2 Drone Specific Examples. Preuzeto sa: https://digital-photography-school.com/aerial-time-lapse-basics-dji-drone/ [Pristupljeno: studeni 2020.]

[2] CNC-STEP: Multicopter design: modelbuilding of a diy y-octocopter, quadrocopter and hexacopter. Preuzeto sa: https://www.cnc-step.com/modelbuilding-multicopter-quadrocopter-hexacopter/ [Pristupljeno: studeni 2020.]

[3] Rc Drone Good: How to make an octocopter? - Homemade octocopter. Preuzeto sa: http://www.rcdronegood.com/how-to-make-octocopter-homemade/. [Pristupljeno: studeni 2020]

[4] Besada, J. A., Bernardos, A. M., Bergesio, L., Vaquero, D., Campana, I., Casar, J. R. *Drones-as-a-service: A management architecture to provide mission planning, resource brokerage and operation support for fleets of drones*. 2019

[5] EASA: Open Category-Civil Drones. Preuzeto sa: https://www.easa.europa.eu/domains/civil-drones-rpas/open-category-civil-drones [Pristupljeno: studeni 2020.]

[6] Unmanned systems technology: Electronic Speed Controllers (ESC). Preuzeto sa https://www.unmannedsystemstechnology.com/expo/electronic-speed-controllers-esc/ [Pristupljeno: siječanj 2020.]

[7] Unmanned systems technology: Flight Control Systems. Preuzeto sa: https://www.unmannedsystemstechnology.com/category/supplier-directory/electronic-systems/flight-control-systems/ [Pristupljeno: studeni 2020.]

[8] Burdziakowski, P.: *Low Cost Hexacopter Autonomous Platform for Testing and Developing Photogrammetry Technologies and Intelligent Navigation Systems.* "Environmental Engineering" 10th International Conference. Vilnius: Gediminas Technical University. Preuzeto sa: https://www.researchgate.net/publication/316646290_Low_Cost_Hexacopter_Autonomous_Platform_for_Testing_and_Developing_Photogrammetry_Technologies_and_Intelligent_Navigation_Systems [Pristupljeno: prosinac 2020.]

[9] Parker Lord: Send in the Drones – 3 Types of Sensors Used in Drones. Preuzeto sa:https://www.microstrain.com/blog/send-in-the-drones-3-types-of-sensors-used-in-drones [Pristupljeno: prosinac 2020.]

[10] Fierce Electronics: How Many Sensors are in a Drone, And What do they Do? Pruezeto sa: https://www.fierceelectronics.com/components/how-many-sensors-are-a-drone-and-what-do-they-do [Pristupljeno: prosinac 2020.]

[11] DJI Enterprise: 6 Ways LiDAR is Revolutionizing Mapping and Geospatial Data. Preuzeto sa: https://enterprise-insights.dji.com/blog/lidar-equipped-uavs [Pristupljeno: prosinac 2020.]

[12] Amazon: DJI Mavic Combo Arctic White. Preuzeto sa: https://www.amazon.com/DJI-Mavic-Combo-Arctic-White/dp/B078WR2TZT [Pristupljeno: prosinac 2020.]

[13] Digital Photo Pro: DJI Mavic Air Hands-On Review Of The Smallest Pro Drone. Preuzeto sa: https://www.digitalphotopro.com/reviews/dji-mavic-air-hands-on-review-of-the-smallest-pro-drone/ [Pristupljeno: prosinac 2020.]

[14] DJI: Mavic AIR Specs. Preuzeto sa: https://www.dji.com/hr/mavic-air/info [Pristupljeno: prosinac 2020.]

[15] Majić, P. Usporedni prikaz forenzičke analize računala i mobilnih uređaja. Fakultet prometnih znanosti, Zagreb, 2018

[16] UFED Logical Analayzer. User Manual, 2014. Pruzeto sa: http://www.mcsira.com/WEB/8888/NSF/Web/3128/UFED%20Logical%20Analyzer2014.pdf [Pristupljeno: prosinac 2020.]

[17] Insectra: Cellebrite UFED Touch 2. Preuzeto sa: https://www.insectraforensics.com/CELLEBRITE-UFED-Touch-2 [Pristupljeno: prosinac 2020.]

[18] Doherty, E.P. *Digital Forensics for Handheld Devices,* 2013

[19] GIGA: Oxygen Forensic Suite 2013. Preuzeto sa: https://www.giga.de/downloads/oxygen-forensic-suite-2013 [Pristupljeno: prosinac 2020.]

[20] Mobiledit: Forensic solutions. Preuzeto sa: http://www.mobiledit.com/forensic-solutions [Pristupljeno: prosinac 2020.]

[21] MSAB: XRY Logical. Preuzeto sa: ://www.msab.com/products/xry/xry-logical/ [Pristupljeno: prosinac 2020.]

[22] MSAB: Prodotti XRY Drones. Preuzeto sa: https://www.msab.com/it/prodotti/xry/drones/ [Pristupljeno: siječanj 2021.]

[23] XRY Drone - access and analyze drone forensic data quickly, MSAB.

[24] Autopsy User Domcumentation: Drone Analyzer. Preuzeto sa: https://sleuthkit.org/autopsy/docs/user-docs/4.14.0/drone_page.html [Pristupljeno: prosinac 2020.]

[25] Sleuthkit: Autopsy. Preuzeto sa: https://www.sleuthkit.org/autopsy/.

[26] AccessData: FTK Imager. Preuzeto sa: https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager [Pristupljeno: siječanj 2021.]

[27] Datfile. Preuzeto sa: https://datfile.net. [Pristupljeno: siječanj 2021.]

[28] AccessData: Drone attacks how can we fight back. Preuzeto sa: https://accessdata.com/blog/drone-attacks-how-can-we-fight-back [Pristupljeno: siječanj 2021.]

[29] Llewellyn, M.: DJI Phantom 3-Drone Forensic data exploration. Joondalup, 2017. Preuzeto sa: https://www.researchgate.net/publication/329879540 _DJI_ Phantom_3-Drone_Forensic_data_exploration [Pristupljeno: siječanj 2021.]

[30] Azhar, H*.: Challenges and Techniques in Drone Forensics*, Canterbury Christ Church University School of Engineering, Technology and Design; 2019. Preuzeto sa: https://www.iaria.org/conferences2019/filesCYBER19/Hannan Azhar_Tutorial_ChallengesAndTechniques.pdf [Pristupljeno: siječanj 2021.]

[31] McMillon, M.: *Building a Low Cost Forensics Workstation*. SANS Institute; 2021. Preuzeto sa https://www.sans.org/reading-room/whitepapers/incident/building-cost-forensics-workstation-895 [Pristupljeno: siječanj 2021.]

[32] Kletuš, T. Forenzička analiza sustava bespilotnih zrakoplova. Fakultet prometnih znanosti, Zagreb, 2020

[33] InformIT: The Anatomy of a Digital Investigation. Preuzeto sa: http://www.informit.com/articles/article.aspx?p=2129764&seqNum=4 [Pristupljeno: siječanj 2021.]

[34] Packtpub.https://www.packtpub.com/sites/default/files/ArticleImages/8311OS_ 01_03.png [Pristupljeno: siječanj 2021.]

[35] Packt: Introduction to Mobile Forensics. Preuzeto sa: https://hub.packtpub.com/introduction-mobile-forensics/ [Pristupljeno: siječanj 2021.]

[36] INFOSEC: The mobile forensics process steps. Pruezeto sa: https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref [Pristupljeno: siječanj 2021.]

[37] MH-Nexus. HxD - Freeware Hex Editor and Disk Editor. Preuzeto sa: https://mh-nexus.de/en/hxd/ [Pristupljeno: siječanj 2021.]

[38] Press Dispensary. Preuzeto sa: https://pressdispensary.co.uk/image_library/q991448.html [Pristupljeno: siječanj 2021.]

[39] Binary Intelligence. Chip-off Forensics. Preuzeto sa: http://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/ [Pristupljeno: siječanj 2021.]

[40] Mahalik, H., Bommisetty, S., Tamma, R.: *Practical Mobile Forensics*, 2016.

[41] DataRecovery: What is JTAG. Preuzeto sa: https://www.datarecovery.co.za/faq/what-is-jtag.html?__cf_chl_jschl_tk__=2e28e1f9546af95148d6a513787d6b2532f36ce2-1614328913-0-Ab0Zv2QTAa5lH_PDzMTv26NQNY7FJpqoo97ii8UmlCXgVnBMCCaTc91dc1p8slT0yTwT55WHXAc63ctrnxslN0sFzH [Pristupljeno: veljača 2021.]

[42] Gillware: JTAG Forensics. Preuzeto sa: https://www.gillware.com/phone-data-recovery-services/jtag-forensics-services/ [Pristupljeno: siječanj 2021.]

[43] Digitpol: Drone Forensic Investigation. Preuzeto sa: https://digitpol.com/drone-forensics/ [Pristupljeno: siječanj 2021.]

[44] Dronexl: DJI Mavic Air 2 teardown video shows h6 processor. Preuzeto sa: https://dronexl.co/2020/05/22/dji-mavic-air-2-teardown-video-shows-h6-processor/ [Pristupljeno: veljača 2021.]

[45] Forensic Focus: Oxygen Drone Forensics. Preuzeto sa https://www.forensicfocus.com/articles/oxygen-drone-forensics/ [Pristupljeno: veljača 2021.]

[46] XDA Developers: What is root for Android. Preuzeto sa https://www.xda-developers.com/what-is-root-for-android/ [Pristupljeno: veljača 2021.]

[47] Oxygen Forensic: Oxygen Forensics Detective. Preuzeto sa: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective [Pristupljeno: veljača 2021.]

[48] Eyewated: Što je SRT datoteka. Preuzeto sa: https://hr.eyewated.com/sto-je-srt-datoteka/ [Pristupljeno: veljača 2021.]

[49] Azdegan, S., Yu, W., Liu, H., Sistani, M.: *Novel Anti-forensics Approaches for Smart Phones*. Towson University; 2012. Preuzeto sa: https://www.researchgate.net/publication/232615931_Novel_Anti-forensics_Approaches_for_Smart_Phones [Pristupljeno: veljača 2021.]

[50] CERT: Steganografija. Preuzeto sa: https://www.cert.hr/wp-content/uploads/2006/06/CCERT-PUBDOC-2006-04-154.pdf [Pristupljeno: veljača 2021.]

[51] Barton, T., Azhar, H.B.: *Open Source Forensics for a Multi-platform*. Canterbury Christ Church University; 2017. Preuzeto sa https://www.researchgate.net/publication/320287487_Open_Source_Forensics_for_a_Multi-platform_Drone_System [Pristupljeno: veljača 2021.]

[52] Maarse, M., Sangers, L.: *Digital forensics on a DJI Phantom 2 Vision+ UAV*. MSc System and Network Engineering, Computer Crime and Forensics, University of Amsterdam; 2016.

[53] Robin Radar Systems: 9 Counter-Drone Technologies To Detect And Stop Drones Today. Preuzeto sa: https://www.robinradar.com/press/blog/9-counter-drone-technologies-to-detect-and-stop-drones-today [Pristupljeno: veljača 2021.]

[54] CISION: Military Grade "NO-DRONE" Counter-UAS Radar Detection System Released for Airport, Facility and Event Anti Drone Protection. Preuzeto sa: https://www.prnewswire.com/news-releases/military-grade-no-drone-counter-uas-radar-detection-system-released-for-airport-facility-and-event-anti-drone-protection-300957178.html [Pristupljeno: veljača 2021.]

[55] Cascade: Drones and Countermeasures. Preuzeto sa: https://cascadeuav.com/2019/04/02/drones-and-countermeasures/ [Pristupljeno: veljača 2021.]

Popis slika

Slika 1. Inačice multikopter bespilotnih zrakoplova 2
Slika 2. Komponente UAS..... 6
Slika 3. Bespilotna letjelica DJI Mavic Air i kontroler..... 8
Slika 4. Forenzički alat Cellebrite UFED Touch 2 13
Slika 5. Sučelje alata XRY Drone..... 15
Slika 6. Autopsy GPS Track..... 16
Slika 7. Prikaz letačkih aktivnosti bespilotne letjelice alatom FTK Quin-C 18
Slika 8. Usporedba brzine ekstrakcije i količine dobivenih podataka 24
Slika 9. Prikaz heksadecimalnog zapisa pomoću Hex preglednika..... 25
Slika 10. Primjena Chip-off metode zagrijavanjem čipa uređaja 26
Slika 11. JTAG ekstrakcija podataka s mobilnog uređaja 27
Slika 12. Unutarnja pohrana bespilotnog zrakoplova DJI Mavic Air 2 29
Slika 13. Proces ekstrakcije podataka pomoću UFED Touch 2 35
Slika 14. Ekstrakcija podataka mobilnog uređaja pomoću uređaja UFED Touch 2. 37
Slika 15. Sažetak informacija o ekstrakciji datotečnog sustava 39
Slika 16. Prikaz sadržaja baze podataka 40
Slika 17. Sažetak informacija o fizičkoj ekstrakciji..... 40
Slika 18. Dohvaćene nekategorizirane datoteke zrakoplova DJI Mavic Air..... 41
Slika 19. Analiza fotografija alatom Physical Analyzer..... 42
Slika 20. Lažno pozitivan ključni dokaz..... 44
Slika 21. Ruta leta tijekom nastanka fotografija 46
Slika 22. Prikaz rute lete i koordinata pomoću alata Oxygen Forensics Detective... 48
Slika 23. Metapodatci fotografije..... 49
Slika 24. Prikaz .SRT datoteke u okviru videozapisa..... 50
Slika 25. Sučelje programa DatCon..... 51
Slika 26. Prikaz podataka nastalih pretvorbom .DAT datoteke 51
Slika 27. Prikaz rute leta i log zapisa 52
Slika 28. Prikaz zapisa leta unutar aplikacije DJI GO 4 52
Slika 29. C-UAS radarski sustav detekcije..... 59

Popis tablica

Tablica 1. Ograničenja za bespilotne zrakoplove bez oznake klase 4
Tablica 2. Tehničke specifikacije DJI Mavic Air bespilotnog zrakoplova 9
Tablica 3. Mogućnosti forenzičkih alata za forenzičku analizu mobilnih uređaja..... 12
Tablica 4. Primjena raznolikih grana forenzike u području forenzike bespilotnih zrakoplova 19
Tablica 5. Mogućnosti forenzičkih alata korištenih u radu 53

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 **Usporedni prikaz alata za postupak forenzičke analize sustava bespilotnih zrakoplova** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 26.2.2021

Student/ica:
Petar Majić
(potpis)