

Analiza mogućnosti prikupljanja podataka i primjene forenzičke analize nosivih terminalnih uređaja

Prgomet, Mario

Master's thesis / Diplomski rad

2019

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:119:810313>

Rights / Prava: [In copyright / Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-04-19**



Repository / Repozitorij:

[Faculty of Transport and Traffic Sciences -
Institutional Repository](#)



SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Mario Prgomet

**ANALIZA MOGUĆNOSTI PRIKUPLJANJA
PODATAKA I PRIMJENE FORENZIČKE ANALIZE
NOSIVIH TERMINALNIH UREĐAJA**

DIPLOMSKI RAD

Zagreb, 2019.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

**ANALIZA MOGUĆNOSTI PRIKUPLJANJA PODATAKA I
PRIMJENE FORENZIČKE ANALIZE NOSIVIH TERMINALNIH
UREĐAJA**

**ANALYSIS OF DATA COLLECTION POSSIBILITIES AND
THE APPLICATION OF FORENSIC ANALYSIS OF
WEARABLE TERMINAL DEVICES**

Mentor: dr. sc. Siniša Husnjak

Student: Mario Prgomet
JMBAG: 0135237354

Zagreb, rujan 2019.

SAŽETAK

Ekspanzijom korištenja nosivih terminalnih uređaja stvara se novo okruženje koje je prošireno putem interoperabilnosti s pametnim mobilnim terminalnim uređajima, čime stvaraju bogat izvor podataka. Upravo takvo okruženje predstavlja izniman izazov u području forenzičke analize. Nosivi terminalni uređaji poput pametnih satova mogu biti vrijedan izvor informacija potrebnih za kriminalističke istrage jer mogu pohraniti određene zapise podataka. Trenutno ne postoji klasifikacija podataka prikupljenih putem nosivih terminalnih uređaja, niti je dostupan popis tehnika za ekstrakciju podataka s određenih vrsta nosivih terminalnih uređaja. Radom je predstavljen proces forenzičke analize koji je proveden nad nosivim i pametnim mobilnim terminalnim uređajem te rezultati ekstrakcije podataka, kako bi se pokazalo koje je podatke moguće prikupiti, a metode koristiti prilikom provedbe forenzičke analize prikupljenih podataka potrebnih u svrhu dokazivanja nezakonitih radnji u pravosudnim postupcima, a jednako tako i u svrhu znanstveno istraživačkih radova.

KLJUČNE RIJEČI: nosivi terminalni uređaji; mobilni terminalni uređaji; digitalna forenzička analiza; ekstrakcija podataka; pametni sat

SUMMARY

The expansion of use of wearable terminal devices creates a new environment that is expanded through interoperability with smart mobile terminal devices whereby creating a rich data source. This is exactly the kind of environment that presents an extraordinary challenge in the field of forensic analysis. Wearable terminal devices such as smartwatches can be a valuable source of information needed for criminal investigations as they can store certain type of data. There is currently no classification of data collected through wearable terminal devices, nor is there a list of techniques for extracting data from specific types of wearable terminal devices. This paper presents the process of forensic analysis that is carried out on a wearable and smart mobile terminal devices and the results of data extraction to show what data can be collected and methods used during conducting a forensic analysis of the collected data for the purpose of proving unlawful acts in judicial proceedings and also for the purpose of scientific research.

KEY WORDS: wearables terminal devices; mobile terminal devices; digital forensic analysis; data extraction; smartwatch

Sadržaj

1. Uvod	1
2. Tehnologija i primjena nosivih terminalnih uređaja	3
2.1. Komunikacijske tehnologije nosivih uređaja	7
2.1.1. Bluetooth	7
2.1.2. Wi-Fi	8
2.1.3. NFC	9
2.1.4. GPS	10
2.1.5. Senzori	12
2.2. Primjena i raznolikost nosivih terminalnih uređaja	14
2.3. Nosivi uređaji kao dio Interneta stvari i implikacije digitalne forenzike	16
3. Forenzička analiza, metode i postupci ekstrakcije podataka	19
3.1. Mobilna forenzika	20
3.2. Izazovi mobilne forenzike	22
3.3. Procedura postupka ekstrakcije dokaza	24
3.4. Metode ekstrakcije	29
3.4.1. Metoda ručne ekstrakcije	30
3.4.2. Metoda logičke ekstrakcije	31
3.4.3. Metoda fizičke ekstrakcije i JTAG metoda	32
3.4.4. Chip-off metoda	33
3.4.5. Micro Read metoda	34
3.4.6. Ostale metode	35
3.5. Antiforenzika	36
4. Forenzički programski alati usmjereni nosivim terminalnim uređajima	38
4.1. Svrha i ograničenja forenzičkih alata	38
4.2. Oxygen Forensic Detective	41
5. Postupak i elementi forenzičke analize nosivih uređaja	43
5.1. Forenzička analiza pametnog mobilnog terminalnog uređaja	45
5.2. Forenzička analiza nosivog terminalnog uređaja	47
6. Analiza ekstrahiranih podataka	49
6.1. Analiza ekstrahiranih podataka s pametnog mobilnog terminalnog uređaja ...	49
6.2. Analiza ekstrahiranih podataka s nosivog terminalnog uređaja	57
6.3. Diskusija o dobivenim rezultatima	59
7. Zaključak	61
Popis literature	62

Popis kratica	66
Popis slika	68
Popis grafikona.....	69
Popis tablica	69

1. Uvod

Zahvaljujući konstantnim inovacijama na području tehnologije današnje doba je doba pametnih uređaja. Najpopularniji i najčešće korišteni suvremeni uređaji su pametni mobilni terminalni uređaji (engl. *smartphone*). Popularni su i široko prihvaćeni zato što su jednostavni za uporabu, potencijalno pružaju nebrojene funkcije i omogućavaju veliku slobodu kretanja prilikom korištenja uređaja. U posljednje vrijeme tehnologija je iznjedrila još jednu novinu, a to je nosiva tehnologija, odnosno pametni uređaji koji se nose na tijelu. To su pametni satovi, pametne narukvice pa čak i pametne majice, tenisice i sl. Iako su dostupni, pristupačni, popularni i vrlo je teško predvidjeti u kojem će se smjeru razvijati - jednako moda kao i tehnologija. Mogućnosti su neograničene.

Pametni mobilni terminalni uređaji, pa tako i nosivi terminalni uređaji (engl. *wearables*), u pravilu bilježe određenu količinu podataka koji mogu biti vrijedan i zanimljiv izvor informacija za terapijska ili znanstvena istraživanja, kao i za forenzička istraživanja povezana s kaznenim djelima. Pametni satovi i fitness narukvice primjeri su vrlo popularnih nosivih terminalnih uređaja koji se koriste širom svijeta. Iako se pametni satovi, za razliku od fitness narukvica, koriste zajedno s nekim drugim pripadajućim pametnim terminalnim uređajima, na njima je, kao samostalnim uređajima, moguće provesti forenzičku analizu. Važno je napomenuti da s rastom broja pametnih nosivih terminalnih uređaja, proporcionalno rastu i kibernetičke zloporabe. Ovdje forenzika kao znanost mora odigrati svoju ulogu.

Danas se aktivno i uspješno provode forenzička istraživanja pametnih mobilnih terminalnih uređaja, no isto se ne može ustvrditi i za nosive terminalne uređaje. Većina komercijalno dostupnih forenzičkih alata jednostavno ne pruža podršku za nosive terminalne uređaje te ih je teško, a katkad i nemoguće identificirati. Kako nosivi terminalni uređaji mogu sadržavati korisne informacije o korisniku, ali podatke koji su zanimljivi za forenzička ispitivanja, razvoj forenzičkih metoda za ispitivanje nosivih terminalnih uređaja je imperativ.

Naslov diplomskog rada je *Analiza mogućnosti prikupljanja podataka i primjene forenzičke analize nosivih terminalnih uređaja*. Cilj je detaljnije prikazati proces forenzičke analize tehnologija nosivih terminalnih uređaja s pripadajućim povezanim mobilnim terminalnim uređajima. Također i utvrditi dostupnosti određenih kategorija podataka, analizirati mogućnosti postupaka forenzičke analize, ali jednako tako istražiti ograničenja koja je potrebno prevladati kako bi se u budućim postupcima dobila cjelokupna forenzička slika.

Rad je podijeljen u sedam cjelina:

1. Uvod
2. Tehnologija i primjena nosivih terminalnih uređaja
3. Forenzička analiza, metode i postupci ekstrakcije podataka

4. Forenzički programski alati usmjereni nosivim terminalnim uređajima
5. Postupak i elementi forenzičke analize nosivih uređaja
6. Analiza ekstrahiranih podataka
7. Zaključak

Poglavlje *Tehnologija i primjena nosivih terminalnih uređaja* definirat će što su to nosivi terminalni uređaji, koje su tehnologije prisutne u uređajima prilikom njihova korištenja te principe njihove primjene u svakodnevnom životu kako bi opravdali status trenutne popularnosti.

Treće poglavlje govori o općenitim značajkama forenzičke analize i mobilne forenzike. Detaljno su obrađene proceduralne faze koje postoje prilikom postupka ekstrakcije dokaza te moguće metode ekstrakcije podataka koje se danas primjenjuju u procesu forenzičke analize.

U četvrtome poglavlju konkretno se opisuju forenzički alati koji se koriste za potrebe provedbe forenzičke analize te se detaljno obrađuje forenzički alat usmjeren forenzičkoj analizi nosivih terminalnih uređaja.

Peto poglavlje obrađuje glavnu stavku diplomskoga rada, a to je postupak forenzičke analize. Postupkom forenzičke analize pokušat će se dobiti uvid u načine i mogućnosti ekstrakcije podataka s korištenih uređaja u kombinaciji s trenutno dostupnim forenzičkim alatima.

U poglavlju *Analiza ekstrahiranih podataka* obrađuju se i analiziraju ekstrahirani podaci prethodno dobiveni procesom forenzičke analize koji su pohranjeni nakon korisničke upotrebe.

2. Tehnologija i primjena nosivih terminalnih uređaja

Pojavom modernih nosivih terminalnih uređaja uslijedila je daljnja modernizacija tehnologije i mogućnost povezivanja fizičkog svijeta s digitalnim okruženjem. Pojam „nosivi“ koristi se u industriji Interneta stvari ili IoT-a (engl. *Internet of Things*), za opisivanje računalnog uređaja koji se može povezati te koji se može implementirati ili nositi na tijelu, [1]. Ovi uređaji obično sadržavaju pametne senzore i povezani su na Internet ili s pripadajućim uređajem radi razmjene podataka. Razne tvrtke, oružane snage i medicinski stručnjaci koriste nosivu tehnologiju već desetljećima, ali se na tržištu za privatne potrošače počela intenzivno pojavljivati tek nedavno, [2].

Stoga, nosiva tehnologija zapravo i nije nova niti je revolucionarno otkriće 21. stoljeća, što će biti navedeno u kratkim povijesnim crtama u nastavku rada. Međutim, prvo se nosivo računalo nije koristilo za poboljšanje kondicije ili zdravlja, po čemu su danas poznati, već za predviđanje ishoda i obavješćavanje subjekta o ishodu igranja kockarske igre - rulet. Važno je napomenuti kako uređaj tehnički nije bio član svijeta IoT-a jednostavno zato što taj pojam kao niti Internet 1955. godine nije postajao, kad je Edward O. Thorp postavio teoriju o prvom nosivom uređaju.

Nosivi uređaji nastavili su sa svojim kontinuiranim razvojem i dalje su se proizvodili, a to su bili uređaji poput kalkulatorskih satova popularnih 1980-ih, digitalnih slušnih pomagala, *Bluetooth* slušalica za telefonske pozive te nekoliko drugih nosivih računala. *Nike+iPod Sport Kit* bio je jedan od prvih uređaja za praćenje atletskih aktivnosti kojega je 2006. predstavila kompanija Nike. Ovaj uređaj sadržavao je mali odašiljač koji je bio postavljen unutar ili na obući osobe te su se informacije prenosile na dostupni uređaj (kao što je *iPod Touch*, *iPhone* ili *iPod nano*). Nadalje, tijekom 2008. na tržištu su se pojavili *Fitbit* uređaji prve generacije. Jedan od takvih uređaja bio je *Fitbit Tracker* koji je mjerio prijeđenu udaljenost, potrošene kalorije i trajanje aktivnosti. Također, kao dodatak praćenju aktivnosti, bila je uključena i funkcija spavanja koja je bilježila i mjerila cikluse spavanja. Sakupljeni podaci na uređaju mogli su se prenijeti na vlastiti korisnički račun na *Fitbit* poslužiteljima, [1].

Prvi pametni sat, *Pebble*, pojavio se na tehnološkoj sceni 2012. godine. U pozadini razvoja uređaja zanimljiva je povijest *Pebblea* (tvrtke Pebble Technology Corporation). Predstavljen svijetu kao kampanja na platformi *Kickstarter*¹, globalnoj zajednici za financiranje kreativnih projekata, navodi se kako će *Pebble* biti u mogućnosti komunicirati s *Android* i *iOS* uređajima, što je prvi uređaj svoje vrste koji pametni sat povezuje s pametnim mobilnim terminalnim uređajima. Iako je proizvod bio kratkog vijeka, tvrtka i intelektualno vlasništvo ovoga proizvoda otkupila je tvrtka Fitbit, u prosincu 2016. za 40 milijuna dolara, što dovoljno govori o potencijalu ovakvih uređaja na tadašnjem tržištu. Godine 2012. Google je objavio novu vrstu nosivog uređaja, a to su nosive naočale pod nazivom *Google Glass*, koje su uključivale opcije kamere i pristupa Internetu. Osoba koja je nosila te naočale mogla je komunicirati s naočalama

¹ *Kickstarter* - globalna zajednica zadužena za financiranje kreativnih projekata

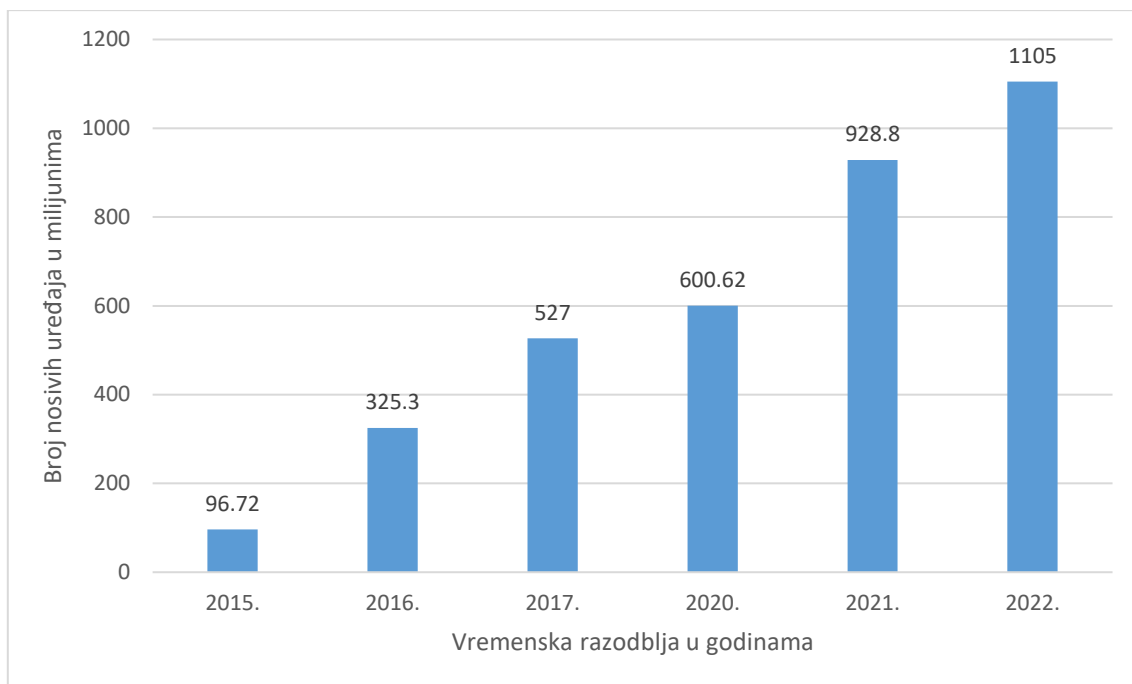
putem glasovnih naredbi kako bi snimila video zapise ili fotografije te pristupala informacijama na internetskim preglednicima i određenim aplikacijama. Ubrzo je postalo jasno da društvo nije spremno za takvu vrstu nosivog uređaja zbog zabrinutosti vezanih uz privatnost korisnika. Aktualne priče o zabrani rada takvog uređaja i ograničenja u njegovu radu, dovela su do toga da je 2015. godine tržište zatvorilo vrata upravo za njih, ali su se u pozadini nastavile i dalje razvijati. Međutim, u 2017. godini, odabrana je nova ciljana grupa korisnika, a to su bila poduzeća. Primjerice, radnici u tvornicama ili industrijskim postrojenjima mogu putem pametnih naočala primati upute vezane uz njihov rad te se to što oni rade može prenositi dalje putem videa, ali važna stavka je ta da im naočale služe i kao sigurnosna oprema. *Google Glas* se na taj način ponovno probio na tržište, što je bilo važno za Google kao tvrtku, ali i za IoT tehnologiju.

U isto vrijeme kada se *Google Glass* prvotno nalazio na tržištu, 2013. godine u prodaju je pušten prvi Samsungov pametni sat pod nazivom *Samsung Galaxy Gear*. Uređaj, zajedno s ostatkom *Gear* serije, omogućuje korisniku primanje obavijesti o aplikacijama, pozivima, porukama i upozorenjima, ali uključuje i zdravstvene aplikacije. Zatim je 2015. godine Apple izdao sat, *Apple Watch*, koji je pomogao da se nosiva tehnologija učini prikladnom te je razvijen s namjerom da ljudi manje vremena provedu gledajući u pametni mobilni terminalni uređaj, ali je i dalje potrebno održavati njihovu međusobnu vezu radi obavijesti, te je tako rođena generacija Appleovih nosivih terminalnih uređaja. *Apple Watch* tako korisnicima omogućuje interakciju s *iPhone* uređajima, primanje poruka, poziva, obavijesti o aplikacijama i mnoge druge opcije, poput serije uređaja *Samsung Gear*. Obje vrste navedenih uređaja komuniciraju putem *Bluetooth* tehnologije s pametnim mobilnim terminalnim uređajima, ali postoji i mogućnost komunikacije putem Wi-Fi veze ukoliko uređaj nije u dometu *Bluetooth* tehnologije. Danas, novi uređaji dolaze s ugrađenom UICC² karticom (engl. *Universal Integrated Circuit Card*) koja omogućuje interakciju s LTE³ (engl. *Long-Term Evolution*) sustavom bez prisustva pametnog mobilnog terminalnog uređaja, [1].

Trenutni trend uporabe nosivih terminalnih uređaja od strane korisnika nije slučajna pošto su se dobro adaptirali i svojom jednostavnošću uklopili u današnji ubrzani ritam čovjekova života. Nosiva tehnologija želi utjecati na razna područja primjene, a primarni joj je cilj ući u svakodnevni život pojedinaca i postati funkcionalni dio u korisničkoj uporabi. Daljnjim napretkom tehnologije i omogućavanjem novih interesantnih opcija za korisnike, taj trend će se nastaviti te će biti popraćen porastom ukupnog broja nosivih terminalnih uređaja u svijetu, što je vidljivo na grafikonu 1. Upravo ovakav rast broja uređaja predstavlja jedan od bitnih izazova u digitalnoj forenzici i to pogotovo u nedovoljno istraženom području poput nosivih terminalnih uređaja.

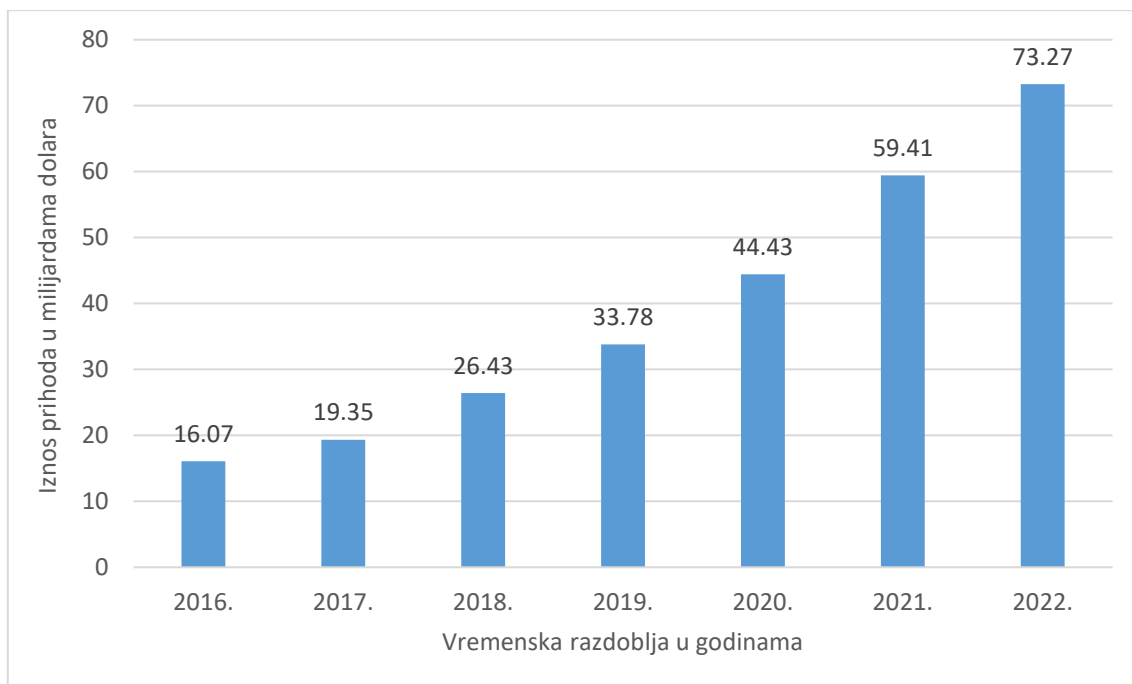
² UICC - vrsta SIM kartice koja se koristi za drugu (GSM) ili treću generaciju (UMTS) mobilne mreže

³ LTE - četvrta generacija mobilnih mreža



Grafikon 1. Statistička analiza broja prodanih nosivih terminalnih uređaja u svijetu
Izvor: [3]

Predviđenim rastom broja nosivih terminalnih uređaja, paralelno će rasti i vrijednost njihova tržišta. Ovisno o načinu kako pojedine projekcije predviđaju vrijednost tržišta bitno je konstatirati da te približne vrijednosti ne odstupaju u velikom broju jedne od drugih. Kako se navodi prema [4], predviđa se da će svjetsko tržište nosivih uređaja 2022. godine vrijediti više od 84 milijarde dolara. Međutim, prema drugoj projekciji [5], kako je prikazano na grafikonu 2, navodi se da će vrijednost tržišta iznositi 73,27 milijarde dolara. U cilju da uzmu svoj udio kolača od predviđene vrijednosti tržišta, tvrtke će morati pažljivo identificirati prilike za učinkovito natjecanje unutar ovoga tehnološkog područja.



Grafikon 2. Prihod od prodaje nosivih terminalnih uređaja u svijetu od 2016. do 2022. godine
Izvor: [5]

Trenutno stanje na tržištu je relativno stabilno i iskazuje se nešto višom prosječnom prodajnom cijenom. U daljnjem razdoblju očekivan je pad prodajne cijene, prvenstveno zbog jeftinih konkurenata na tržištu, ali i stvaranja zalihosti što uzrokuje manju proizvodnju, kao i zbog smanjenja cijena komponenti. Jake će tvrtke, kao što su Apple i Samsung, pokušati zadržati stabilnost cijena svojih tradicionalnih brendova. S vremenskim odmakom, segment pametnih satova dalje će se nastaviti razvijati i usavršavati te će se podijeliti u četiri glavne vrste pružatelja usluga: vodeće robne marke potrošačke elektronike, modne i tradicionalne brendove, dječje satove te specijalizirane marke i startup-ove koji pružaju usluge ciljanoj publici poput ljudi s medicinskim potrebama koje je potrebno nadzirati, [6].

2.1. Komunikacijske tehnologije nosivih uređaja

Primjenom nosivih uređaja u raznim područjima potrebne su određene tehnologije koje mogu osigurati povratne informacije o stanju na uređaju, koje su prikupljene u određenom trenutku, te ostvariti potrebnu komunikaciju između uređaja sa svrhom razmjene pripadajućih podataka. U primjere takvih tehnologija korištenih unutar nosivih terminalnih uređaja, koje će u nastavku rada detaljnije biti objašnjene, prema [7] spadaju sljedeće:

- *Bluetooth*
- Wi-Fi
- NFC
- GPS
- razni senzori.

2.1.1. Bluetooth

Bluetooth jedan je od najpopularnijih standarda bežične komunikacije kratkog dometa, [8]. Namijenjen je zamijeni korištenja kablova koji međusobno povezuju elektroničke uređaje. Ključne karakteristike *Bluetooth* bežične tehnologije su robusnost, mala potrošnja energije i niski troškovi proizvodnje. Također je poznat i pod nazivom standarda IEEE⁴ (engl. *Institute of Electrical and Electronics Engineers*) 802.15.1, a mnoge karakteristike osnovne verzije specifikacije navode se kao izborne što omogućava razlikovanje proizvoda. Stvoren je od strane telekomunikacijskog dobavljača Ericsson 1994. godine te je prvotno zamišljen kao bežična alternativa podatkovnim kablovima tipa RS-232 (engl. *Recommended Standard 232*). Godine 1998. tvrtke Ericsson, IBM, Intel, Nokia i Toshiba osnovali su trgovinsko udruženje poznato kao *Bluetooth SIG* (engl. *Special Interest Group*) radi objavljivanja i promocije *Bluetooth* standarda, [9].

Bluetooth tehnologija djeluje unutar frekvencijskog opsega 2,4 GHz te omogućava bežične mreže uskog područja kako bi se omogućila komunikacija u rasponu udaljenosti od 10 metara (što vrijedi za *Bluetooth* uređaje klase II i klase III) i više od 100 metara za uređaje klase I, koji se uglavnom koriste u industrijskoj primjeni. S novim mrežnim i modulacijskim shemama, čak su i uređaji klase II i klase III s malom snagom sposobni pokriti područje dometa veće od 10 metara. SIG kontinuirano mijenja i nadograđuje *Bluetooth* specifikacije kako bi bili u toku s potražnjom i u koraku s razvojem tehnologije i njezinim potrebama. Potrošačima nadogradnje *Bluetooth* standarda donose brojne prednosti poput veće sigurnosti, više funkcionalnosti (npr. poboljšana brzina prijenosa podataka), racionalnija potrošnja električne energije i pouzdanosti pri uparivanju uređaja. Generacija *Bluetooth* 1.x suočila se s brojnim implementacijskim i sigurnosnim problemima u tadašnje vrijeme te je sada zastario. *Bluetooth* 2.x otvorio je vrata za masovno usvajanje standarda, poboljšanu

⁴ IEEE - Institut inženjera elektrotehnike i elektronike, neprofitna stručna udruga

interoperabilnost između uređaja i brzo uparivanje te je uveo poboljšanje u vidu brzine prijenosa podataka. *Bluetooth 3.x* obilježen je oznakom velike brzine tako što se nadodala podrška protokolu veze nižeg sloja na kojem bi se sve *Bluetooth* mogućnosti mogle pokrenuti s alternativne opcije na uređaju poput Wi-Fi opcije. Konačno, *Bluetooth 4.x* uveo je nisko-energetsku podršku za uređaje poput nosivih terminalnih uređaja i pametnih senzora s niskim potrebama prijenosa podataka. Postoje dva oblika *Bluetooth* bežične tehnologije: *Basic Rate/Enhanced Data Rate* (BR/EDR) i *Low Energy* (LE) sustavi, [10].

Oba sustava uključuju opcije poput otkrivanja uređaja, uspostavljanja konekcije i mehanizme pomoću kojih se konekcija uspostavlja. LE sustav zapravo je nadogradnja BR sustava te uključuje dizajnirane značajke koje omogućuje proizvodnju proizvoda koji zahtijevaju manju potrošnju energije, nižu kompleksnost i niže troškove proizvodnje od BR sustava. Također, LE sustav dizajniran je za uporabu i aplikacije s nižom brzinom prijenosa podataka i nižim radnim ciklusima, a važno je napomenuti da je prvenstveno napravljen kako bi se *Bluetooth* tehnologija mogla implementirati u uređaje koje su pokretani od strane malih plosnatih baterija nalik novčiću, upravo kao što su razni primjeri nosivih terminalnih uređaja poput pametnih satova. Ključni tehnološki ciljevi *Bluetooth* LE sustava uključuju manju potrošnju energije, manju potrebu za zahtjevima memorije, učinkovite postupke otkrivanja uređaja i povezivanja, slanju kratkih duljina paketa u komunikaciji te jednostavne protokole i usluge, [9].

2.1.2. Wi-Fi

Wi-Fi predstavlja tehnologiju bežičnog umrežavanja koja uređajima kao što su računala (prijenosna i stolna računala), mobilni terminalni uređaji (pametni mobilni terminalni uređaji i nosivi terminalni uređaji) i ostala oprema (pisači, videokamere itd.) omogućuje povezivanje s Internetom. Uz to, navedenim uređajima također pruža i mogućnost međusobne razmjene informacija stvaranjem svojevrsne komunikacijske mreže, [11]. Također se navodi da je upravo Wi-Fi najčešće korištena tehnologija bežične komunikacije i predstavlja primarni medij za globalni internetski promet, [12].

Kao zaštitni znak organizacije Wi-Fi Alliance⁵, a ne akronim, Wi-Fi je jedan od nekoliko IEEE bežičnih protokola iz 802.11 obitelji standarada (što se osobito odnosi na protokole 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac te 802.11ax). Tehnički gledano, to su sve izmjene i dopune izvornog standarda 802.11, ali su i sami *de facto* objavljeni kao samostalni standardi. Ono po čemu se standardi međusobno razlikuju su različite frekvencije rada, isporuke količine propusnosti i podržan broj kanala, [13], [14].

Tradicionalno, Wi-Fi je koristio frekvencijski pojas od 2,4 GHz, koji se upotrebljavao u industrijske, znanstvene i medicinske svrhe. Iako je protokol 802.11a koristio frekvencijski pojas od 5 GHz, 802.11n podržava to kao moguću opciju odabira, dok se

⁵ Wi-Fi Alliance - neprofitna organizacija koja objedinjuje svjetske tvrtke radi promoviranja Wi-Fi tehnologije

802.11ac ponovno vraća isključivo na 5 GHz, [14]. Novi posljednji protokol 802.11ax, koji bi se u upotrebi trebao pojaviti u posljednjem kvartalu 2019. godine, ponovno ima mogućnost frekventijskog pojasa 2,4 ili 5 GHz, [15]. U tablici 1. sažeto su prikazane osnovne karakteristike prethodno navedenih verzija Wi-Fi tehnologije.

Tablica 1. Osnovne karakteristike verzija Wi-Fi tehnologije

IEEE naziv	Max. brzina prijenosa podataka	Frekvencijski pojas	Širina kanala	Novi naziv
802.11a	54 Mbps	5 GHz	20 MHz	/
802.11b	11 Mbps	2.4 GHz	20 MHz	/
802.11g	54 Mbps	2.4 GHz	20 MHz	/
802.11n	65-150 Mbps	2.4 ili 5 GHz	20-40 MHz	Wi-Fi 4
802.11ac	78-867 Mbps	5 GHz	20-160 MHz	Wi-Fi 5
802.11ax	Do 1200 Mbps	2.4 ili 5+ GHz	20-160 MHz	Wi-Fi 6

Izvor: [14]

Frekvencijski pojas od 5 GHz ima smanjenu sposobnost prodiranja kroz zidove, što često rezultira nižim efektivnim dometom, ali pruža mogućnost korištenja više kanal nego pojas od 2,4 GHz što u konačnici dovodi do mnogo manje smetnji u prenapučenom okruženju uređaja. No problem predstavlja to što radio frekvencijski spektar Wi-Fi tehnologije nije licenciran te ne treba posebna dozvola za njegovo korištenje, što može uzrokovati da netko drugi istovremeno koristi isti frekvencijski pojas, [14].

2.1.3. NFC

Near Field Communication tehnologija, poznatija pod akronimom NFC, oblik je beskontaktna komunikacije bliskog polja između uređaja kao što su pametni mobilni terminalni uređaji ili nosivi uređaji. Princip rada beskontaktna komunikacije ove tehnologije omogućuje korisniku da svojim pripadajućim uređajem, u cilju slanja ili prihvata informacija, prijeđe preko NFC kompatibilnog uređaja bez potrebe za njihovim međusobnim dodirivanjem ili prolazanjem kroz postupke potrebne procedure koja bi bila potrebna za uspostavu konekcije. Tehnologija NFC-a svoje korijene vuče iz RFID (engl. *Radio Frequency Identification*) tehnologije. NFC se zapravo očituje kao podskup RFID tehnologije, ali s karakteristikom kraće komunikacijske udaljenosti kojom je pridodan značaj sigurnosnom aspektu upotrebe ove tehnologije, [16].

NFC, *Bluetooth* i Wi-Fi, međusobno posjeduju pojedine sličnosti kao tehnologije. Sve tri navedene tehnologije omogućuju bežičnu komunikaciju i razmjenu podataka između digitalnih uređaja. Međutim, NFC koristi elektromagnetsko polje, dok se *Bluetooth* i Wi-Fi koriste radio frekvencijom. Uređaji koji koriste NFC tehnologiju mogu biti pasivni ili aktivni. Pasivni uređaji, kao što su NFC oznake⁶, u sebi samo sadrže i pohranjuju informacije koje drugi uređaji mogu čitati. Suprotno pasivnim uređajima su

⁶ NFC oznake - informacijski objekti koje NFC kompatibilni uređaj može obraditi i pročitati

aktivni uređaji koji mogu pročitati dostupne informacije i prema mogućnostima proslijediti ju dalje i podijeliti s drugim kompatibilnim uređajima. Također, ako je aktivan uređaj predstavljen kao ovlašten uređaj, može promijeniti podatke koji se nalaze unutar NFC oznaka, [17]. Da bi se osigurala sigurnost, NFC često uspostavlja sigurnosni kanal za komunikaciju i koristi se enkripcija prilikom slanja osjetljivih podataka, kao što su brojevi kreditnih kartica, upravo zato što je beskontaktno plaćanje sve popularniji način za novčane transakcije i plaćanja, [17], [18].

Unutar NFC tehnologije postoje razni standardi koji moraju biti ispunjeni kako bi sve forme pripadajuće tehnologije bile usklađene i kompatibilne u interakciji s uređajima baziranim na ovakvoj vrsti tehnologije te da u budućnosti mogu raditi s novim uređajima. Kao dvije glavne specifikacije prema [19] navode se: ISO/IEC 14443 te ISO/IEC 18000-3. Prvi spomenuti, ISO/IEC 14443, definira identifikacijske iskaznice koje se koriste za pohranu informacija te ih je moguće pronaći unutar jedne NFC oznake. Druga specifikacija, ISO/IEC 18000-3, određuje RFID komunikacije koje se koriste od strane NFC uređaja te predstavlja međunarodni standard za sve uređaje čija je komunikacija bežična i radi na frekvenciji od 13,56 MHz. Definirano je da uređaji međusobno moraju nalaziti na udaljenosti od 4 cm prije nego što je moguće započeti prenositi informacije. Standard također objašnjava način kako uređaj i NFC oznaka međusobno trebaju provoditi komunikaciju, u čijem je slučaju uređaj poznat kao predajnik, a sama NFC oznaka kao prijatelj.

2.1.4. GPS

Globalni položajni sustav ili GPS (engl. *Global Positioning System*), satelitski je radionavigacijski sustav za pružanje neprekidnih informacija i određivanje položaja na Zemlji ili u njezinoj blizini, [20]. Razvijen 1970-ih godina pod okriljem Ministarstva obrane Sjedinjenih Američkih Država, GPS je izvorno bio namijenjen prvenstveno u vojne svrhe, radi pružanja informacija o navigaciji, lokaciji i vremenu za vojne operacije, [21].

1980-ih godina učinili su ga dostupnim za javnu civilnu upotrebu. Znanstvena primjena GPS-a se povećavala iz dana u dan na području vojnih, civilnih i komercijalnih korisnika te zahvaljujući razvoju tako dolazi do povećanja produktivnosti u raznim područjima gospodarstva. Glavne komunikacijske mreže, navigacija, bankarski sustavi, tržišta i elektroenergetske mreže ovise o GPS-u radi preciznog vremenskog usklađivanja, dok neke bežične usluge ne mogu funkcionirati bez njega. Tako američki navigacijski sustav u svijetu nije jedini te postoje i ostali drugačiji navigacijski sustavi koji su upotrebi ili se nalaze u određenim fazama razvoja, a u radu [20] navedeni su idući:

- NAVSTAR - *Navigation System with Time And Ranging Global Positioning System*, Sjedinjene Američke Države, u potpunosti operativan diljem svijeta i najkorišteniji u civilnoj uporabi

- GLONASS - *Globalnaja Navigacionaja Sputnjikova Sistema* ili *Global Navigation Satellite System*, Rusija, u potpunosti operativan diljem svijeta
- GALILEO - kao ime poznatog astronoma, globalni sustav razvijen od strane Europske unije i ostalih partnerskih zemalja, dok se prema navodima na službenim stranicama potpuna operativna sposobnost očekuje tokom 2020. godine, [22]
- BEIDOU - regionalni sustav Narodne Republike Kine koji je dostupan globalnom korištenju
- IRNSS - *Indian Regional Navigation Satellite System*, Indija, predstavlja regionalni navigacijski sustav koji pokriva područje Indije i sjever Indijskog oceana te postoje planovi za daljnje proširenje
- QZSS - *Quasi-Zenith Satellite System*, Japan, također regionalni sustav koji pokriva Aziju i Oceaniju.

GPS koncept temelji se na vremenu, tj. na mjerenju vremena potrebnom za propagaciju signala od satelita do prijemnika. Sateliti sadrže vrlo stabilne i precizne atomske satove koji su međusobno sinkronizirani te osiguravaju potrebnu stabilnost signala i usklađenost s jedinstvenim GPS vremenom. GPS prijemnici također imaju satove, ali nisu sinkronizirani u stvarnome vremenu i manje su stabilni pa tako GPS sateliti neprekidno prenose svoje trenutačno vrijeme i položaj. GPS prijemnik nadzire više satelita i rješava jednadžbe kako bi utvrdio točan položaj prijemnika i njegovo odstupanje od stvarnog vremena, [20], [23].

GPS sustav sastoji se od dvije vrste sustava. Postoji precizan sustav pozicioniranja koji koristi Ministarstvo obrane Sjedinjenih Američkih Država i njihove oružane snage te je vrlo precizan. Zatim postoji standardni sustav pozicioniranja koji se često naziva i GPS civilnog stupanja koji nije precizan kao prethodno navedeni, [24]. GPS tehnologija i njezina primjena mogu se prikazati putem tri velike cjeline GPS-a gdje se prema [20] navode sljedeće:

1. svemirski segment - sastoji se od satelita i odašiljanih signala
2. kontrolni segment - sastoji se od zemaljskih stanica koje osiguravaju da sateliti ispravno rade
3. korisnički segment - sastoji se od prijemnika u uređajima korisnika.

Svemirski segment sastoji se od barem 24 satelita, koji kruže oko Zemlje u orbitama na visini od oko 20.000 km. Sateliti su raspoređeni unutar šest orbitalnih ravnina odabranih tako da se u svakom trenutku iznad horizonta nalazi barem 5 ili više satelita, čime se postigla globalna pokrivenost. Sateliti emitiraju signale na dvjema prijenosnim frekvencijama na koje se moduliraju kodovi za pozicioniranje i navigacijske poruke. Kontrolni segment obavlja nadzor i upravlja cjelokupnim sustavom. Kontrolne stanice raspoređene su po čitavom svijetu i kontinuirano prate sve GPS satelite i prosljeđuju primljene satelitske signale u glavnu kontrolnu postaju gdje se izračunavaju odstupanja njihovih atomskih satova od GPS vremena. Izračunate korekcijske veličine za svaki pojedini satelit, šalju se satelitima nekoliko puta na dan gdje su ti izračuni uključeni u

navigacijsku poruku. U slučaju nepredviđenih situacija, primjerice da satelit izgubi kontakt s kontrolnim sustavom, satelit tako može raditi samostalno nekoliko mjeseci. U korisničkome segmentu postoje dvije kategorije korisnika: autorizirani korisnici, poput američke vojske i neautorizirani korisnici, u koje spadaju svi ostali korisnici širom svijeta, [20], [23]. Daljnja smanjivanja veličine GPS prijemnika odnosno njihova minijaturizacija dovela je do toga da se njima opremaju mobilni terminalni uređaji, ali isto tako i nosivi terminalni uređaji.

2.1.5. Senzori

Senzori su sofisticirani uređaji koji se često koriste za otkrivanje i reagiranje na mehaničke, električne ili optičke signale. Senzor ima ulogu pretvaranja fizičkog parametra u signal pogodan za daljnju obradu (najčešće u električni signal) i mjerenje. Postoje razne vrste senzora koji se klasificiraju prema prirodi izmjerene veličine te se prema [25] navode sljedeći:

- toplinski senzori - koriste se za mjerenje temperature, toplinskog kapaciteta i toplinskog izgaranja
- mehanički senzori - koriste se za mjerenje sile, tlaka, vakuuma i mehaničkog naprezanja
- kinematički senzori - koriste se za mjerenje linearnog i kutnog ubrzanja te brzine protoka
- geometrijski senzori - koriste se za mjerenje položaja i razine tijela
- radijacijski senzori - koriste se za mjerenje intenziteta toplinskog, nuklearnog, akustičnog i elektromagnetnog zračenja te boje parametara valnog procesa
- vremenski senzori - koriste se za mjerenje vremena i frekvencije
- električni senzori - koriste se za mjerenje elektromotorne sile, struje, otpora induktivnosti, kapaciteta i vodljivosti
- kemijski senzori - koriste se za mjerenje kemijskog sastava
- fizikalni senzori - koriste se za mjerenje mase, gustoće, vlažnosti, tvrdoće i hrapavosti.

Senzori rade na osnovu njihove interakcije s procesom i to tako što reagiraju na registrirana stanja, a reakciju transformiraju u izlazni signal. Postoji velik broj fizikalnih pojava i efekata, načina transformacije svojstava procesa, kao i metoda pretvaranja energije koji se mogu primijeniti pri kreiranju senzora. Nosilac informacije je masa ili energija. Mjerenje neelektričnih signala počinje pretvaranjem u električni pa se onda obavlja procesiranje. Važnost imaju fizikalni efekti koji omogućavaju takvu konverziju. Za neelektrično-električno pretvaranje potrebna je energija iz domena mjernog signala ili van njega. Većina mjernih pretvornika sastoji se od tri osnovna dijela:

1. izvora informacija ili senzora
2. mjernog sustava ili adaptera
3. podsustava za predstavljanje informacija ili ekrana.

Senzor se još naziva primarnim elementom. Ovaj dio koristi energiju posebnog izvora u cilju stvaranja veličine koja predstavlja izmjerenu vrijednost. U sekundarnom elementu ili adapteru vrši se obrada signala iz primarnog elementa. Podsustav za predstavljanje informacija, ekran ili izlazni element je dio mjernog pretvornika koji na razne načine iznosi rezultate mjerenja. Pretvaranje neelektričnih mjernih veličina u električne vrši se pomoću odgovarajućih pretvarača na dva moguća načina. Prvi način podrazumijeva da se odgovarajuća neelektrična veličina pretvara u pretvaraču u električnu veličinu. Pretvarači koji rade na ovaj način zovu se aktivni pretvarači te oni za svoj rad ne trebaju dodatnu energiju. Drugu grupu pretvarača čine pasivni pretvarači ili parametarski pretvarači. U pasivnim pretvaračima neelektrične veličine utječu na promjenu neke električne karakteristike (kapaciteta, otpora ili induktivnosti), [25]. Senzori prikupljaju podatke i prenose ih u procesorsku jedinicu ili CPU (engl. *Control Processing Unit*) gdje se dalje obrađuju, [26].

Senzori su osnova nosivih terminalnih uređaja i osnovno su sredstvo na kojemu se očituju ulazni podaci. Senzori za nosive uređaje razlikuju se od onih za druge mobilne terminalne uređaje i proizvode, jer nude jedinstvene značajke po kojima su upravo nosivi uređaji zanimljivi korisnicima. Lokacija pojedinih senzora unutar nosivih terminalnih uređaja prikazana je slikom 1, dok se senzori nosivih uređaja prema [26] se mogu podijeliti u sljedeće tri kategorije i pripadajuće senzore:

1. senzori pokreta

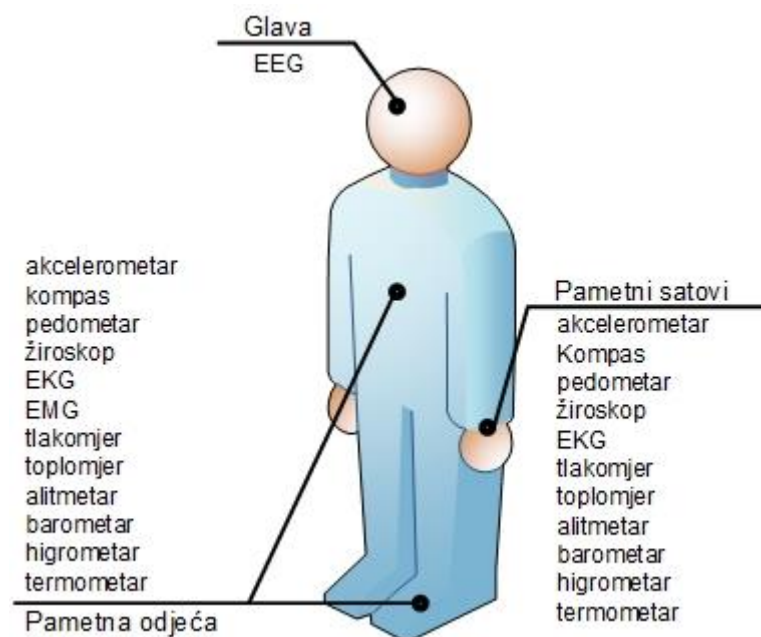
- akcelerometar - uređaj za mjerenje akceleracije (ubrzanja)
- geomagnetski senzor (kompas) - uređaj koji reagira na geomagnetska polja Zemlje
- pedometar - uređaj koji registrira i broji korake osobe otkrivajući gibanje
- žiroskop - instrument za mjerenje ili održavanje orijentacijske brzine

2. bio-senzori

- EEG - elektroencefalogram, elektrode koje očitavaju električnu aktivnost moždanih stanica (neurona)
- EKG - elektrokardiogram, elektrode koje prikazuju električnu aktivnost srčanih otkucaja
- EMG - elektromiografija, elektrode kojima se mjeri električna aktivnost određenih mišića i živaca
- glukometar - uređaj za mjerenje razine glukoze
- tlakomjer - uređaj za mjerenje krvnog tlaka
- toplomjer - instrument za mjerenje temperature tijela osobe

3. okolišni senzori

- alitmetar - uređaj za određivanje visine
- barometar - instrument za mjerenje tlaka zraka
- higrometar - instrument za mjerenje vlažnosti
- termometar - instrument za mjerenje temperature.



Slika 1. Senzori nosivih terminalnih uređaja

Kako će se tehnologija i dalje razvijati, senzori će poprimati sve manje dimenzije te će biti pametniji, precizniji, a potrošnja energije će im se dodatno smanjiti, [26]. Prvi val senzora koji su bili ugrađivani u nosive uređaje pojavili su se prije desetak godina te su izvorno bili razvijeni za nosive proizvode, dok su danas praktički postali samostalna industrija. Nakon toga je uslijedio drugi val nosivih senzora, koji je nastupio uz ogromna ulaganja u pametne mobilne terminalne uređaje i njihovom pojavom na tržištu. Tada se pojavila ideja da bi se senzori s pametnih mobilnih terminalnih uređaja mogli lako prilagoditi i upotrijebiti unutar novih uređaja koji bi bili nosivi uređaji. U konačnici, kako su nosive tehnologije i određena ulaganja dosegla vrhunac, mnoge organizacije identificirale su određene tipove senzora koji bi se mogli razvijati posebno prema namjeni nosivih uređaja. Uz činjenice kako nosivi terminalni uređaji postaju sve napredniji, uvodeći više vrsti senzora, upravo uloga senzora postaje izrazito važna jer oni služe za prikupljanje podataka i daju potrebno razumijevanje za budući razvoj i previđanje potencijala ove industrije.

2.2. Primjena i raznolikost nosivih terminalnih uređaja

Prethodno spomenutom minijaturizacijom komponenti sadržanih unutar nosivih terminalnih uređaja, a isto tako i samih uređaja, pojavljuju se nove i velike mogućnosti njihove primjene u raznim područjima. Zapravo, različiti načini izvedbe i mogućnosti prilagodbe pogoduju određenim područjima u kojima se pokazuju kao interesantni objekti za implementaciju. Upravo takva raznolikost njihove upotrebe, koja je poprimila veliki opseg, dovela je do toga da ih je teško precizno kategorizirati u jednu skupinu te se prema raznim izvorima kategorizacija različito tumači.

Autor u radu [27] postavlja detaljnu podjelu nosivih terminalnih uređaja, koji su svrstani u sljedeće kategorije te su kategorije dodatno pojašnjene tablicom 2:

- prema industriji namjene
- prema vrsti proizvoda
- prema lokaciji uređaja na tijelu korisnika.

Tablica 2. Kategorička podjela nosivih terminalnih uređaja

Industrija namjene	Vrsta proizvoda	Tjelesna lokacija uređaja
• Zdravstvena skrb i medicina • Sportska industrija • Komercijalna industrija • Industrija općenito • Vojna industrija • Više sektorska industrija • Druga industrija	• Pametni satovi • Sportska i fitness oprema • Pametne narukvice na ručnim zglobovima, sportski prsluci ili grudnjaci, modni dodaci (npr. pametne naušnice) • Pametne naočale • Uključuju tehnologiju virtualne stvarnosti (VR) i proširene stvarnosti (AR), pametne kontaktne leće • Pametna odjeća • Uključuje odjeću široke potrošnje, sportsku, medicinsku, modnu i vojnu odjeću, odjeću za nadzor pri radnim aktivnostima • Medicinski uređaji • Raščlamba prema bolesti npr. dijabetes (senzori), kardiovaskularni tretmani i nadzor, kontaktne leće, slušni aparati, neurološki uređaji, dijagnostički uređaji • Ostali uređaji	• Glava • Uši • Oči • Tijelo/torzo • Ruke • Zglobovi ruke • Noge i stopala • Implantirani uređaji • Više lokacijski • Prilagodljivi uređaji prema korisniku ili potrebama uporabe

Izvor: [27]

Sportski sektor relativno je rano prihvatio tehnologiju u svome području i postoje razna rješenja visoke tehnologije koje se nalaze u primjeni te se takav status ranog prihvaćanja ne može se primijeniti za komercijalnu pametnu nosivu odjeću. Međutim, većina sportova bazira se na koristi od gubitka mase u sportaševoj opremi, pa je dodavanje elektronike u početku bio velik problem. Ipak, nosivi uređaji su napredovali te su se prilagodili potrebama sportaša zahvaljujući velikim ulaganjima na području sporta i danas su svakodnevica u sportskim okruženjima. Kategorija sportske odjeće također se može podijeliti na skupine ovisno o tome radi li se o profesionalnom i natjecateljskom ili običnom rekreativnom sportu, pri čemu svaka kategorija zasebno koristi drugačiju tehnologiju. U profesionalnim vodama koriste se biofizičke tehnologije i senzori za praćenja koji se preklapaju sa zdravstvenim nadzorom, dok se za rekreaciju koristi odjeća s ugrađenim zabavnim ili komunikacijskim tehnologijama. Isto tako postoji mnogo nosivih tehnoloških rješenja za medicinski nadzor. Obično su dizajnirani samo s jednom namjenom, a to je uzeti očitavanja s određenih područja na tijelu, što se danas obično postiže vrlo učinkovito. Praćenje tijela najpreciznije je kada se vrši u potpunom kontaktu s kožom. Međutim, ovi su uređaji često neugodni,

neugledni i nespretni za upotrebu, izazivajući pacijentima osjećaj nelagode i smanjenje želje za korištenjem uređaja. Medicinski zdravstveni proizvodi imaju veći naglasak za stalno praćenje biofizičkih podataka kao što su primjerice EKG, brzina disanja, krvni tlak, temperatura i kretanje. Ovo je jasna korist uređaja koji se nose na tijelu, posebno u slučajevima kada je potreban dugotrajni nadzor. S druge strane, ako bi se osobni, tjelesni instrumenti mogli očitavati i analizirati na daljinu, i liječnici i njihovi pacijenti mogli bi uštedjeti vrijeme i novac uz manje rutinske posjete. Medicinsko ispitivanje ovih proizvoda je neophodno jer svaka država ima svoja vlastita pravila i zahtjeve za kliničkim testiranjima koje je potrebno postići prije nego što se proizvod može koristiti u kliničkom okruženju. To je često važan faktor za tvrtke koje razvijaju takve uređaje, jer to može uzrokovati visoke financijske izdatke za testiranje proizvoda. Nekoliko tvrtki u početku je ciljano radilo za sportsku industriju, a kasnije su prešli na medicinsku industriju jer su njihovi proizvodi daljnjim razvojem postigli razinu točnosti i konzistentnosti koje su potrebne za kliničku upotrebu. Postoje dvije glavne vrste zdravstvenih proizvoda: one koje propisuje liječnik (medicinska zdravstvena zaštita) ili one koje kupuju pojedinci koji se brinu za vlastito opće zdravstveno stanje, [28], [29].

Vojna industrija u početku bila je jedan od najvećih izvora financijskih sredstava za razvoj nosivih uređaja i pripadajućih tehnologija. Američka vojska bila je posebno aktivna u razvoju pametne nosive odjeće i nosivih tehnoloških rješenja pa su tako u programu NATICK krenuli s razvijanjem posebnih odjelnih oklopa za vojnike, a odijelo bi uključivalo inteligentni oklop, nadzor biofizičkih podataka, oružje, komunikacije i egzoskelet, [29]. Kako se mnogi nosivi proizvodi povećavaju i s vremenom propadaju te prolaze kroz krivulju zasićenosti, tvrtke se konsolidiraju oko aspekata nosivih proizvoda koji dodaju najviše vrijednosti te se okreću njihovoj proizvodnji i plasiranju na tržištu. U mnogim slučajevima podloga tih vrijednosti upravo potječe od podataka iz senzora, [27].

2.3. Nosivi uređaji kao dio Interneta stvari i implikacije digitalne forenzike

Internet stvari (engl. *Internet of Things*) paradigma je koncepta koji se pojavljuje posljednjih godina iako je Kevin Ashton koncept IoT-a uveo još 1999. godine. Koncept se opisuje kao širok sustav u kojem međusobno povezani uređaji i usluge prikupljaju, razmjenjuju i obrađuju podatke kako bi svoju međusobnu komunikaciju dinamički prilagodili kontekstu njihove uporabe. IoT danas je definiran kao kibernetičko-fizički sustav međusobno povezanih senzora i uređaja koji omogućuju inteligentno odlučivanje. Iz tih navoda upravo proizlazi važnost informacija, koje su bitna stavka i nalaze se u središtu samoga sustava i time su od iznimnog značaja za funkcioniranje sustava kao jedinstvene cjeline Interneta stvari. U IoT okruženjima, „stvar“ predstavlja fizički ili virtualni objekt kojeg je moguće identificirati i integrirati u komunikacijske mreže. Neophodno je da objekti IoT-a imaju mogućnost komunikacije tj. mogućnost razmjene podataka putem komunikacijskih mreža između njih. Uz to, stvari mogu imati i druge neobavezne značajke, kao što su očitavanje, pokretanje, pohranjivanje i obrada podataka, izvršavanje izvornih aplikacija itd. Skupom objekata koje čine IoT okruženje

može se upravljati putem inteligentnih sustava koji se mogu autonomno povezati s objektima radi nadgledanja i kontrole. Štoviše, ovi inteligentni sustavi mogu preuzeti podatke iz nekog zasebnog objekta ili skupa objekata i obraditi te podatke, čime će se dobiti korisne informacije za donošenje inteligentne odluke, [30].

Prema mišljenju pojedinih autora nosivi terminalni uređaji smatraju se dijelom Interneta stvari. Iako ta teza nije globalno prihvaćena, ostali autori ih smatraju jedinstvenom i samostalnom cjelinom odnosno samo nosivim uređajima bez da spadaju u bilo kakvu drugu kategoriju. Međutim, tako se u radovima [30], [31] i [32] navodi kako su nosivi terminalni uređaji dio Interneta stvari i zbog čega se ubrajaju u to područje. S kasnijim vremenskim odmakom i cijenom napretka tehnologije koja je uzrokovala smanjenje veličine hardverskih komponenata, dostupnost senzora, njihove niske cijene i troška proizvodnje te postojanje široko rasprostranjenog pristupa Internetu omogućili su da nosivi terminalni uređaji postanu uobičajeni, lako nosivi i društveno prihvatljivi. To energično širenje minijaturnih računalnih uređaja dovelo je do koncepta Interneta stvari koji je danas u sve većoj uporabi te tako međusobno povezani i interaktivni uređaji komuniciraju i dijele korisne informacije u stvarnome vremenu. Pametni satovi, kao vrsta nosivih terminalnih uređaja, spadaju u kategoriju Interneta stvari te djeluju kao periferni uređaj povezanom pametnom mobilnom terminalnom uređaju. Međusobnim uspostavljanjem veze između pametnog sata i pametnog mobilnog terminalnog uređaja, moguće je jednostavno upravljati i koristiti pametni mobilni uređaj putem pametnog sata, [31].

Nadalje, senzori se navode kao jedan od ključnih i osnovnih elemenata Interneta stvari budući da kao sastavni elementi omogućavaju praćenje okolišnih događaja i konteksta u kojem IoT sustavi djeluju. Na fizičkoj razini senzori mogu mjeriti definirane fizičke, kemijske ili biološke pokazatelje, što je prethodno bilo detaljnije opisano, dok na digitalnoj razini prikupljaju informacije o mreži i aplikacijama. Veličina senzora tj. njihove dimenzije, koje mogu biti veličine milimetra, upravo je jedan od glavnih razloga što ih čini jednostavnim za ugradnju u fizičke objekte. Umjesto da posjeduju vlastite senzorske mreže, IoT uređaji mogu se naći i kao ugrađeni sustavi, koji uključuju ugrađene senzore, kao i mrežne mogućnosti za izravno povezivanje s Internetom. Uz to, IoT ugrađeni sustavi temelje se na procesorskoj jedinici koja im omogućuje samostalnu obradu podataka, a kao primjer uređaja koji sadrže ugrađene sustave navode se pametni satovi kao jedni od nosivih terminalnih uređaja koji sadrže razne senzore ovisno o potrebama korisnika i njihovoj namjeni, [30].

Smatranjem nosivih terminalnih uređaja dijelom Interneta stvari donosi niz jedinstvenih i složenih izazova na području digitalne forenzike. Kako bi se iskoristila količina i raznolikost prikupljenih te pohranjenih podataka u sveprisutnim IoT uslugama, forenzički istražitelji trebaju se poslužiti metodama i tehnikama prikupljanja dokaza iz svih područja digitalne forenzike i eventualno stvoriti nove procese i načine istrage specifične za IoT okruženje. Iako je razvijen niz konceptualnih modela procesa provedbe istrage koji se bave jedinstvenim karakteristikama IoT-a, mnogi izazovi ostaju neriješeni. Znanost digitalne forenzike usredotočena je na podržavanje istraga

digitalnih uređaja uključujući i one koji se nalaze IoT okruženju. Digitalna forenzika oslanja se na digitalne dokaze, znanstveno izvedene i dokazane metode prikupljanja dokaza i potvrđene forenzičke alate koje koriste kvalificirani forenzički stručnjaci kojima je u cilju olakšati pribavljanje podataka i analizu forenzički ispravnih digitalnih dokaza koji se u kasnijim sudskim procesima mogu iznijeti i priznati.

Upravo je nastanak IoT-a donio brojne izazove pred digitalnu forenziku, posebno zahtijevajući da se trenutne metode i tehnike primjenjuju u vrlo raznolikom i stalno promjenjivom digitalnom okruženju. Pojavljivanje IoT-a doživljava se kao potencijalni pokretač novina u procesu digitalne forenzičke istrage. Na primjer, podaci koje prikupljaju i dijele sveprisutni senzori predstavljaju obilje potencijalnih digitalnih dokaza zahvaljujući njihovom broju, raznolikosti i pokrivenosti u mnogim područjima primjene. Digitalni artefakti pronađeni u IoT sustavima mogu se upotrijebiti za potporu ili pobijanje hipoteza tijekom provođenja procesa forenzičke istrage. Međutim, složenost koja se temelji na izvlačenju podataka iz IoT infrastrukture i njenih uređaja može ometati sposobnost istražitelja za stvaranje forenzički ispravnih i prihvatljivih dokaza, [33].

Prvenstveno se radi prethodno navedenih razloga diplomski rad bazira na nosivim terminalnim uređajima. Zbog postojanja potencijala u otkrivanju novih mogućnosti procesa forenzičke analize i ekstrahiranih podataka te mogućih inovativnosti u području nosivih terminalnih uređaja, a sve zbog toga jer postaju lako dostupni i pristupačni te je stoga nužno provoditi više istraživanja pripadajućih vrsta uređaja.

3. Forenzička analiza, metode i postupci ekstrakcije podataka

Podaci pohranjeni i stvoreni na uređajima predstavljaju dvosjekli mač iz forenzičke perspektive, pružajući uvjerljive dokaze u širokom rasponu istraga, ali i uvodeći složenost koja može utjecati na cjelokupan proces forenzičke analize. Forenzička analiza predstavlja proces identifikacije, prikupljanja, obrade i analize podataka različitim dostupnim i primjenjivim metodama ovisno o potrebama samog procesa. U novije vrijeme, sve aktualnija je digitalna forenzička analiza koja je identična definiciji forenzičke analize i grana je forenzičke znanosti, ali sa svrhom i fokusom na opravak, prikupljanje i analizu digitalnih dokaza iz elektroničkih ili digitalnih uređaja posredstvom informacijsko komunikacijskih tehnologija, [34], [35].

Ekstrakcija podataka postupak je prikupljanja podataka s medija koji ih sadrži u svrhu daljnje obrade i pohrane. Razlozi ekstrakcije podataka s mobilnih terminalnih uređaja mogu biti različiti kao i tehnike koje se koriste za njihovu obradu. Ponekad su za istragu važni samo određeni podaci, dok se u drugim slučajevima radi cjelokupna ekstrakcija datotečnog sustava i/ili fizičke memorije uređaja za potrebe potpunog forenzičkog ispitivanja i potencijalnog oporavka izbrisanih podataka, [36].

Pod digitalnim dokazima podrazumijevaju se podaci ili informacije koje se pohranjuju, obrađuju ili prenose određenim elektroničkim uređajem te kao takvi imaju izniman značaj u forenzičkoj analizi, [34]. Digitalni dokazi obuhvaćaju sve digitalne podatke koji se mogu koristiti kao dokaz u slučaju predmeta istrage, [35].

Upravo se digitalni dokazi mogu koristiti kao odgovor na temeljna pitanja koja se odnose na kriminalističke istrage, uključujući ono što se dogodilo, kada se to dogodilo, tko je s kime komunicirao (određivanje povezanosti), podrijetlo određenih predmeta i tko je bio odgovoran. Istovremeno, složenost sustava obuhvaćenih forenzičkom analizom zahtijeva razumijevanje da pojedinačni dijelovi digitalnog dokaza mogu imati višestruke interpretacije, a potkrepljujuće informacije mogu biti od vitalne važnosti za postizanje ispravnog zaključka. Da bi se digitalni dokazi maksimalno iskoristili, forenzički istražitelji trebaju razumjeti i redovito se služiti znanstvenom metodom. Znanstvena metoda koja se primjenjuje zajedno s metodologijama i tehnikama digitalne forenzike omogućava prilagodbu različitim okolnostima i zahtjevima u pojedinim slučajevima, ali i osigurava da doneseni zaključci sadrže čvrste temelje. Usvojeni postupci u provedbi digitalne forenzike izravno utječu na ishod istrage te odabir neprimjerenih istražnih postupaka može dovesti do nepotpunih ili nedopuštenih dokaza što rezultira da odgovorne osobe za počinjena kaznena djela ili kriminalne aktivnosti neće odgovarati pred licem pravde te će sudski postupak i istraga protiv njih biti odbačeni, [34].

Upravo izraz „forenzički prihvatljivo ili zvučno“ (engl. *forensically sound*) predstavlja izraz je koji se široko koristi u zajednici digitalne forenzike da bi se kvalificirala i opravdala upotreba partikularne forenzičke tehnologije ili metodologije. Glavni princip zdravog forenzičkog istraživanja digitalnih dokaza je da se izvorni dokazi ne smiju mijenjati, [35].

Proces forenzičke analize tako uključuje uzimanje činjeničnih opažanja iz dostupnih dokaza, formiranje i testiranje mogućih objašnjenja za ono što je prouzročilo dokaze te na kraju stvaranje dubljeg razumijevanja određenih kaznenih dijela ili kriminalnih aktivnosti u cjelini. Drugim riječima, elementi digitalne forenzičke analize uključuju odvajanje pojedinih predmeta za pojedinačno istraživanje, određivanje njihove važnosti i razmatranje kako se oni odnose na čitav spektar dokaza. Taj postupak često uključuje eksperimentiranje i istraživanje te može dovesti do dodatnih informacija koje se moraju sintetizirati u cjelokupan proces. Primjerice, analizom je moguće predložiti dodatne stavke koje je potrebno istražiti kako bi se pronašle dodatne informacije koje će pridonijeti detaljnijem i daljnjem procesu forenzičke analize. Kao takav, proces je ciklički definiran pa je moguć višestruki ponovni prolazak kroz određene faze cjelokupnog procesa. Općenitije, forenzička analiza uključuje objektivno i kritičko ocjenjivanje digitalnih dokaza kako bi se shvatilo i došlo do zaključaka o zločinu. Ovaj postupak može uključivati procjenu izvora digitalnih objekata, istraživanje nepoznatih formata datoteka radi izdvajanja korisnih informacija, razvijanje vremenskih rokova za prepoznavanje slijeda i obrazaca u vremenu događaja, provođenje funkcionalne analize kako bi se utvrdilo što je moguće i nemoguće te relacijske analize za utvrđivanje odnosa i interakcije između komponenata zločina. U osnovi, forenzički istražitelji pokušavaju odgovoriti na temeljna pitanja u istrazi što se dogodilo, gdje, kada, kako te tko je bio sudionik i zašto, [34].

3.1. Mobilna forenzika

Pametni mobilni terminalni uređaji danas su kompaktni oblici računala visokih performansi, ogromne pohrane i poboljšanih funkcionalnosti. Pametni mobilni terminalni uređaji predstavljaju najosobniji elektronički uređaj kojem korisnik pristupa. Koriste se za obavljanje jednostavnih komunikacijskih zadataka i potreba, poput pozivanja i slanja poruka, dok još uvijek pružaju podršku za internetsko pregledavanje, e-poštu, fotografiranje i videozapise, stvaranje i spremanje dokumenata, identificiranje lokacija s GPS uslugama i upravljanje poslovnim zadacima, [35].

Uz pametne mobilne terminalne uređaje povezuju se i nosivi terminalni uređaji, koji mogu biti interesantan izvor dokaza u procesu forenzičke analize. Iako je njihovo područje u procesu forenzike relativno novo i neistraženo, pokazuju izniman potencijal upravo zbog sličnih karakteristika koje dijele s mobilnim terminalnim uređajima te su s njima međusobno povezani. Kako se nove značajke i aplikacije uključuju u pametne mobilne terminalne uređaje, upravo količina podataka pohranjenih na uređajima neprestano raste. Uz sve veću sigurnosnu zaštitu, podaci dobiveni iz pametnim mobilnih terminalnih uređaja postaju neprocjenjivi izvor dokaza za kriminalističke

istrage. Rijetkost je da je potrebno provesti digitalnu forenzičku istragu koja ne uključuje mobilni terminalni uređaj.

Mobilna forenzika je znanost koja se temelji na povratu i analizi digitalnih dokaza iz mobilnih terminalnih uređaja i predstavlja jednu od grana digitalne forenzike. Kako je ranije navedeno da je glavni princip zdravog forenzičkog istraživanja digitalnih dokaza taj da se izvorni dokazi ne smiju mijenjati, to je izuzetno teško postići s mobilnim terminalnim uređajima. Neki forenzički alati zahtijevaju komunikacijski vektor s mobilnim terminalnim uređajem, dok ostale metode forenzičke akvizicije mogu uključivati uklanjanje čipa ili instaliranje zasebne aplikacije za pokretanje na uređaju prije mogućeg početka ekstrakcije podataka u svrhu forenzičke istrage. U slučajevima kada prikupljanje podataka nije moguće bez promjene konfiguracije uređaja, svaki postupak promjene konfiguracije mora biti testiran, potvrđen i dokumentiran domenom određene metodologije. Potrebno je slijediti odgovarajuću metodologiju i smjernice jer su od presudnog značaja za forenzičku istragu i ispitivanje mobilnih terminalnih uređaja radi toga jer mogu dati iznimno vrijedne podatke. Kao i kod svakog prikupljanja dokaza, nepoštivanje odgovarajućeg postupka tijekom procesa istrage može rezultirati gubitkom ili oštećenjem dokaza što će kasnije biti odbačeno u sudskim procesima, [35].

Mobilna forenzika podijeljena je u tri glavne kategorije: oduzimanje, pribavljanje i analiza. Forenzički istražitelji suočavaju se s mnogim izazovima dok preuzimaju mobilni terminalni uređaj kao izvor dokaza. Na mjestu zločina, ako se utvrdi da je mobilni terminalni uređaj isključen, istražitelj treba uređaj staviti u Faradayevu vrećicu kako bi se spriječile eventualne promjene u slučaju da se uređaj automatski uključi. Faradayeve vrećice posebno su dizajnirane vrećice za izoliranje terminalnog uređaja s mogućim povezivanjem na mrežu. Ako je telefon zaključan PIN-om ili lozinkom, istražitelj će trebati zaobići sigurnosno zaključavanje ili odrediti točnu uzorak načina zaključavanja da bi pristupio uređaju. Mobilni terminalni uređaji umreženi su uređaji te mogu slati i primati podatke putem različitih izvora kao što su razni telekomunikacijski sustavi tj. mobilne mreže, Wi-Fi, *Bluetooth* itd. Dakle, ako je telefon u ispravnom stanju, zločinac ili treća osoba u mogućnosti je sigurnosno izbrisati podatke pohranjene na telefonu izvršavajući naredbu putem opcije udaljenog brisanja podataka. Kad je telefon uključen, treba ga staviti u Faradayevu vrećicu. Prije mogućnosti stavljanja mobilnog terminalnog uređaja u Faradayevu vrećicu, potrebno ga je isključiti iz mreže na način da mu se omogući zrakoplovni način rada te mu se tako onemoguće sve mrežne veze. Nakon što je mobilni terminalni uređaj pravilno preuzet i obrađen, istražiteljima će trebati nekoliko forenzičkih alata da bi napravili ekstrakciju i analizu podatka pohranjenih na samome uređaju, [34], [35].

Mobilni terminalni uređaji dinamični su sustavi koji pred forenzičke istražitelje stavljaju mnoštvo izazova pri ekstrakciji i analizi digitalnih dokaza. Brz porast broja različitih vrsta mobilnih terminalnih uređaja od različitih proizvođača značajno otežava razvoj jedinstvenog postupka ili alata za ispitivanje svih vrsta uređaja. Mobilni terminalni uređaji kontinuirano se razvijaju kako napreduju postojeće tehnologije, ali i

kako se uvode nove tehnologije. Nadalje, svaki je mobilni terminalni uređaj opremljen s drugačijim ugrađenim operativnim sustavom te zbog tih razloga od stručnjaka na području forenzike zahtijevaju posebna znanja i vještine u svrhu provedbe forenzičke analize. Forenzička analiza mobilnih terminalnih uređaja može se provesti putem više metoda, koje će biti definirane u nastavku rada. Svaka od navedenih metoda utječe na količinu ekstrahiranih podataka te ako jedna od primijenjenih metoda ne uspije, potrebno je pokušati drugu, [35].

3.2. Izazovi mobilne forenzike

Jedan od najvećih forenzičkih izazova kada su u pitanju mobilne platforme je činjenica da se podacima može pristupiti putem drugog uređaja, a isto tako moguće je podatke pohraniti i sinkronizirati na te iste uređaje. Kako su podaci nestabilni i mogu se brzo transformirati ili izbrisati na daljinu, za očuvanje tih podataka potrebno je uložiti veliki napor. Mobilna forenzika razlikuje se od računalne forenzike i predstavlja jedinstvene izazove forenzičkim istražiteljima. Provoditelji zakona i forenzički istražitelji često se bore za pribavljanje digitalnih dokaza s mobilnih terminalnih uređaja. Autori u [35] navode neke od razloga:

- **Razlike hardvera** → tržište je preplavljeno različitim modelima mobilnih terminalnih uređaja različitih proizvođača. Forenzički istražitelji nailaze na različite verzije određenih modela mobilnih terminalnih uređaja koji se razlikuju u veličini, hardveru, značajkama i operativnom sustavu. Također, važno je napomenuti da se zbog kratkog ciklusa razvoja proizvoda vrlo često pojavljuju novi modeli mobilnih terminalnih uređaja. Kako se tržište mobilnih terminalnih uređaja mijenja svakoga dana i poprima sve veću širinu, za istražitelje je presudno da prihvate sve izazove vezane uz to područje i budu ažurni po pitanju forenzičkih tehnika koje se primjenjuju za mobilne terminalne uređaje.
- **Operativni sustavi za mobilne uređaje** → za razliku od osobnih računala na kojima Windows godinama dominira tržištem, mobilni uređaji koriste više različitih operativnih sustava, uključujući: *iOS (Apple)*, *Android (Google)*, *BlackBerry OS (RIM)*, *Windows Mobile (Microsoft)*, *webOS (HP)*, *Symbian OS (Nokia)* i mnoge druge.
- **Sigurnosne značajke mobilne platforme** → moderne mobilne platforme sadrže ugrađene sigurnosne značajke za zaštitu korisničkih podataka i privatnosti korisnika. Ove značajke djeluju kao prepreka tijekom forenzičke akvizicije i istraživanja. Primjerice, pametni mobilni terminalni uređaji dolaze sa zadanim mehanizmima za enkripciju⁷ od hardverskog do softverskog sloja. Forenzičkim istražiteljima možda će biti potrebno probiti ove mehanizme šifriranja kako bi ekstrahirali podatke iz uređaja.
- **Nedostatak resursa** → kao što je ranije spomenuto, ubrzanim porastom broja mobilnih terminalnih uređaja, alati koje zahtjeva forenzička analiza i potrebni su

⁷ Enkripcija - ili šifriranje, metoda kojom se podaci konvertiraju u kodirani oblik koji nije razumljiv neautoriziranim korisnicima

forenzičkim istražiteljima također bi se trebali proporcionalno povećavati. Oprema za forenzičku akviziciju uređaja, poput USB (engl. *Universal Serial Bus*) kabela, baterija i punjača za različite mobilne terminalne uređaje, moraju se održavati i redovito nabavljati kako bi se omogućila akvizicija na uređaje.

- **Generičko stanje uređaja** → čak i ako se čini da je uređaj u isključenom stanju, još se uvijek mogu izvoditi pozadinski procesi. Primjerice, na pametnim mobilnim terminalnim uređajima, alarm će i dalje raditi iako je uređaj isključen. Nagli prijelazi iz jednog stanja u drugo, može rezultirati izmjenom podataka.
- **Antiforenzičke tehnike** → kao što su skrivanje podataka, krivotvorenje podataka, sigurnosno brisanje podataka, izravni napadi na alate i tehnike digitalne forenzike.
- **Dinamička priroda dokaza** → digitalne dokaze moguće je lako mijenjati namjerno ili nenamjerno. Primjerice, pregledavanje određene aplikacije na mobilnom terminalnom uređaju može izmijeniti podatke pohranjene u toj aplikaciji na uređaju.
- **Slučajno resetiranje** → pametni mobilni terminalni uređaji nude različite opcije za resetiranje uređaja i vraćanje na tvorničke postavke. Slučajno resetiranje uređaja tijekom postupka provedbe forenzičke analize može rezultirati gubitkom podataka.
- **Izmjene na uređaju** → mogući načini izmjena na uređaju mogu se okarakterizirati pokušajima premještanja podataka aplikacije, preimenovanja datoteka i izmjene operativnog sustava proizvođača uređaja. U ovom je slučaju potrebno uzeti u obzir stručnost i znanje osumnjičenih osoba.
- **Oporavak lozinke** → ako je uređaj zaštićen lozinkom ili PIN-om, forenzički istražitelji moraju pristupiti uređaju bez oštećivanja postojećih podataka na uređaju.
- **Zaštita komunikacije** → mobilni terminalni uređaji komuniciraju putem mobilne mreže, Wi-Fi mreže, *Bluetooth* tehnologije i sl. Kako je putem komunikacija na uređaju moguće izmijeniti podatke o i na uređaju, nakon oduzimanja i daljnjeg procesuiranja uređaja potrebno je ukloniti mogućnosti za daljnju komunikaciju.
- **Nedostatak dostupnih alata** → iako postoji širok raspon mobilnih terminalnih uređaja, moguće je da jedan forenzički alat ne podržava sve uređaje ili ne obavlja sve potrebne funkcije u procesu forenzičke analize, tako da je u tom slučaju poželjno i treba koristiti kombinaciju više alata. Upravo odabir pravog forenzičkog alata za određeni telefon može biti iznimno težak korak pri započinjanju procesa forenzičke analize.
- **Zlonamjerni programi** → mobilni terminalni uređaj može sadržavati zlonamjerne programe poput virusa⁸ ili trojanskog napada⁹. Takvi se

⁸ Virus - samoumnažajući program kojemu je glavni cilj promijeniti način rada uređaja, bez znanja i dopuštenja korisnika

⁹ Trojanski napad - vrsta zlonamjernog programa koji je maskirani kao legitimni programi ili je njihov programski kod ugrađen unutar legitimnih programa

zlonamjerni programi mogu pokušati proširiti na druge uređaje putem žičane ili bežične komunikacije.

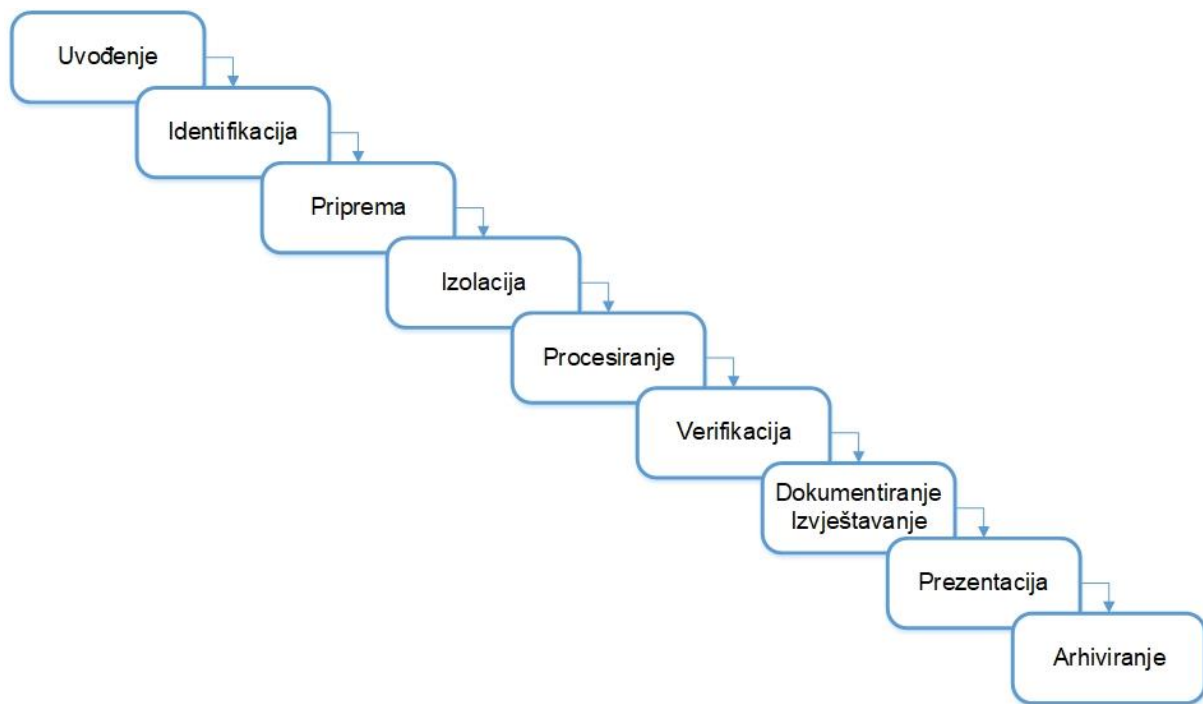
- **Pravni problemi** → mobilni terminalni uređaj mogao bi biti dokaz u kriminalističkim istragama i povezan sa zločinom. Tako postoji mogućnost da se zločin dogodio na nekoj drugoj lokaciji tj. izvan granica matične države u kojoj se uređaj nalazi. Da bi se forenzički istražitelji mogli pozabaviti tim pitanjima potrebno je poznavati jurisdikciju međunarodnih institucija.

3.3. Procedura postupka ekstrakcije dokaza

Uz rastuću potražnju za istragama i provođenjem forenzičke analize nad pametnim mobilnim terminalnim uređajima i drugim mobilnim uređajima, pojavila se i potreba za razvojem smjernica u vezi ispitivanja ovih uređaja. Procesi izvlačenja dokaza i forenzičkih istraživanja za svaki pojedini mobilni terminalni uređaj mogu se razlikovati. Međutim, iako se specifični detalji istraživanja pojedinih uređaja razlikuju, usvajanje dosljednih postupaka istraživanja i metodologije pomoći će forenzičkim istražiteljima u osiguravanju da dokazi ekstrahirani iz svakog mobilnog terminalnog uređaja budu dobro dokumentirani te da su rezultati ponovljivi i vjerodostojni.

Razmotrena i dobro definirana metodologija rada omogućuje provedbu istrage korak po korak. Uostalom, postoji velik broj metodologija i određeni će se forenzički istražitelji držati pojedinih metoda. Sve metode koje se koriste pri ekstrakciji podataka s mobilnih uređaja trebaju biti testirane, potvrđene i dobro dokumentirane. Naime, problem koji nastaje radi velikog broja metodologija je taj da postupci forenzičke istrage nisu konzistentni i ne postoji obaveza provođenja određene procedure u svrhu istrage veće se to navodi kao preporuka koju bi bilo dobro slijediti. Također, valja napomenuti kako proces provođenja istrage ovisi o nadležnoj zakonskoj regulativi.

U svijetu ne postoji jedinstveno uspostavljen i standardiziran postupak za mobilnu forenziku. Zbog toga je razvoj smjernica i procesa za ekstrakciju i dokumentiranje podataka s mobilnih terminalnih uređaja izuzetno važan. Upravo se smjernice i procesi moraju konstantno i pravovremeno preispitivati jer se tehnologija mobilnih terminalnih uređaja i dalje razvija i mijenja, [35], [36]. Na sljedećoj slici, slika 1, prikazan je proces ekstrakcije dokaza s mobilnih terminalnih uređaja ili CPEEP (engl. *Cellular Phone Evidence Extraction Process*) koji se sastoji od devet koraka.



Slika 2. Faze procedure postupka ekstrakcije dokaza
Izvor: [35]

Faza uvođenja

Faza uvođenja započinje zaprimanjem zahtjeva za istragom ili samoga uređaja kao dokaznog materijala. Unutar ove faze pregledavaju se obrasci zahtjeva za istragom i ispunjava se dokumentacija o općim informacijama o vlasništvu uređaja, lancu posjedovanja dokaza i vrsti incidenta u kojemu je uređaj sudjelovao te se iznose opće informacije o vrsti podataka ili informacija koje su tražene nalogom za istragu. Ključ ove faze je razraditi specifične ciljeve istrage, [35], [36].

Faza identifikacije

Unutar faze identifikacije forenzički istražitelji trebali bi utvrditi sljedeće detalje vezane uz svako ispitivanje mobilnog terminalnog uređaja:

- pravna ovlaštenja za ispitivanje uređaja
- ciljeve istraživanja
- proizvođača, model i identifikacijske podatke o uređaju
- ostale izvore potencijalnih dokaza.

Važno je da forenzički istražitelj utvrdi i dokumentira pravna ovlaštenja koja postoje za akviziciju i ispitivanje uređaja, kao i sva ograničenja koja su postavljena na istragu prije same akvizicije (analiza svih podataka na uređaju ili samo onih obuhvaćenih nalogom). Ciljevi istraživanja čine značajnu stavku prilikom odabira metoda i forenzičkih alata za analizu mobilnog terminalnog uređaj i povećavaju efikasnost cjelokupnog postupka forenzičke analize, [35], [36].

U sklopu forenzičke analize prepoznavanje proizvođača tj. marke i modela mobilnog uređaja uvelike pomaže u određivanju koji će forenzički alati najoptimalnije funkcionirati prilikom akvizicije na uređaj. Ovisno o tehnologiji mobilnog terminalnog uređaja, postoje dodatne identifikacijske informacije koje je potrebno dokumentirati ako su dostupne, poput oznaka:

- ESN (engl. *Electronic Serial Number*) → elektronički serijski broj, jedinstveni 32-bitni identifikacijski broj decimalnog ili heksadecimalnog zapisa koji se nalazi ispod baterije ili na stražnjoj strani uređaja
- MEID (engl. *Mobile Equipment Identifier*) → identifikator mobilnog opreme, globalni jedinstveni 56-bitni identifikacijski broj decimalnog ili heksadecimalnog formata te je zamijenio ESN
- IMEI (engl. *International Mobile Equipment Identity*) → međunarodni identifikator mobilnog uređaja, jedinstven 15-bitni broj za identifikaciju mobilnog uređaja u mobilnoj mreži koji se nalazi ispod baterije uređaja
- IMSI (engl. *International Mobile Subscriber Identity*) → međunarodni identifikator mobilnog pretplatnika, jedinstven 15-bitni broj za identifikaciju koji je dodijeljen svakom mobilnom pretplatniku GSM¹⁰ sustava
- MSISDN (engl. *Mobile Station International Subscriber Directory Number*) → međunarodni telefonski broj pretplatnika mobilne stanice, jedinstven broj koji se sastoji od 15 znamenki za identifikaciju mobilnog broja.

Isto tako mobilni terminalni uređaji djeluju kao dobra podloga izvora otisaka prstiju i drugih bioloških dokaza. Takve dokaze potrebno je prikupiti prije daljnjeg postupka ispitivanja uređaja kako bi se izbjegao problem njihove kontaminacije i zbog toga se istražiteljima preporučuje nošenje rukavica prilikom manipuliranja uređajem, [35], [36].

Faza pripreme

Nakon identifikacije mobilnog terminalnog uređaja, faza pripreme uključuje istraživanje i pripremu samoga uređaja koji se ispituje i traženje odgovarajućih metoda i alata koji će se primjenjivati prilikom akvizicije uređaja i analize, [35].

Faza izolacije

Mobilni terminalni uređaji dizajnirani su tako da komuniciraju putem mobilnih telefonskih mreža, *Bluetooth* tehnologije, Wi-Fi mreža itd. Kad je mobilnom terminalnom uređaju dozvoljena mogućnost spajanja na bilo kakvu komunikacijsku mrežu, u uređaj se dodaju novi podaci te se isti pohranjuju, a novi podaci mogu biti generirani putem dolaznih poziva, poruka, programa i aplikacija, što uzrokuje promjenu dokaza na samome uređaju. Potpuno uništenje podataka tj. njihovo brisanje na uređaju također je moguće putem naredbi za udaljeni pristup uređaju ili daljinsko brisanje podataka. Iz tog razloga, izolacija uređaja od komunikacijskih mrežnih izvora iznimno je važna prije ikakvih daljnjih koraka u procesu forenzičke analize i pregledavanja uređaja. Izolacija mobilnog terminalnog uređaja može se postići

¹⁰ GSM - druga generacija digitalnog globalnog sustava mobilne mreže

korištenjem Faradayevih vrećica, koje blokiraju radio frekvencijske signale prema uređaju ili one koje bi sam uređaj odaslao prema mreži. Određena istraživanja otkrila su pojedine nedosljednosti u komunikacijskoj zaštiti tj. izolaciji uređaja primjenom Faradayevih vrećica stoga je preporučljivo i zasebno izoliranje mobilnog terminalnog uređaja iz mreže. To je moguće postići postavljanjem uređaja u omot previđen za zaštitu od radio frekvencijskih signala te naknadnim postavljanjem opcija na uređaju u zrakoplovni način rada, [35].

Faza procesiranja

Kada je tijekom prethodne faze mobilni terminalni uređaj izoliran od utjecaja komunikacijskih mreža, u fazi procesiranja započinje stvarna obrada uređaja. Na uređaj je tako potrebno izvršiti akviziciju testiranom metodom koju je moguće kasnije ponoviti te da je ona što je moguće više „forenzički prihvatljiva ili zvučna“. Poželjna metoda za primjenu je fizička akvizicija, jer ona izvlači neobrađene memorijske podatke dok je uređaj obično isključen tijekom postupka akvizicije. Na većini uređaja dolazi do najmanjih mogućih izmjena tijekom fizičke akvizicije. U slučaju ako fizička akvizicija nije moguća ili postupak ne uspije, potrebno je pokušati steći pristup datotečnom sustav mobilnog terminalnog uređaja. Također, uvijek je potrebno izvršiti i logičku akviziciju jer je moguće da će rezultati sadržavati samo raščlanjene podatke što će pružiti smjernice za ispitivanje neobrađenih memorijskih podataka, [35].

Faza verifikacije

Nakon obrade mobilnog terminalnog uređaja, istražitelj mora provjeriti točnost tj. verificirati podatke ekstrahirane iz uređaja kako bi se osiguralo i potvrdilo da podaci nisu bili podložni nikakvim izmjenama. Provjeru ekstrahiranih podataka moguće je provesti na više načina:

- usporedbom ekstrahiranih podataka i izravnim pregledom podataka na uređaju
- korištenjem više forenzičkih alata i međusobnom usporedbom njihovih rezultata
- korištenjem *hash*¹¹ vrijednosti.

Provjeravanjem podudarnosti ekstrahiranih podataka s podacima na uređaju iznimno je delikatna način zbog toga jer rukovanje uređajem može promijeniti originalni dokaz tj. sam uređaj. Podaci se mogu usporediti izravnim pregledom podataka na uređaju ili putem logičkog izvješća kako bi se utvrdilo odgovaraju li ekstrahirani podaci s uređaja podacima koje uređaj prikazuje. Za bolje osiguranje točnosti potrebno je koristiti više forenzičkih alata za ekstrakciju podataka i usporedbu rezultata, međutim ovisno o mogućnostima alata postoji vjerojatnost da neće svi ekstrahirati jednaku količinu podataka, ali podaci koji su im jednaki trebali bi pokazati međusobnu podudarnost. Nadalje, svaka ekstrahirana stavka trebala bi sadržavati *hash* vrijednost kako bi se osiguralo da su ti podaci ostali nepromijenjeni. Ako je tijekom procesa ekstrakcije ekstrahiran datotečni sustav uređaja, forenzički istraživač nakon ekstrakcije

¹¹ *Hash* vrijednost - format ireverzibilne tj. jednosmjerne enkripcije, cilj je identifikacija originalnih podataka kako bi se dokazalo da nisu promijenjeni u bilo kojem smislu

izračunava *hash* vrijednosti za izvađene datoteke. Kasnije se u postupku svaka *hash* vrijednost pojedinačno izračunava i provjerava u odnosu na izvornu vrijednost da bi se provjerila njegova cjelovitost. Svako odstupanje u *hash* vrijednosti mora imati odgovor na pitanje zašto se to dogodilo. Primjerice, ako se uređaj uključi i ponovi se postupak akvizicije na uređaj, *hash* vrijednost pokazat će odstupanja od originalne vrijednosti, [35].

Faza dokumentiranja i izvještavanja

Forenzički istražitelj dužan je dokumentirati sve korake u obliku zapisnika koje se odnose na ono što je učinjeno za vrijeme trajanja cjelokupnog procesa forenzičke analize uređaja. Nakon što istražitelj završi istragu, rezultati moraju proći kroz neki oblik stručnog pregleda i mišljenja kako bi se osigurala provjera priloženih podataka i utvrdilo da je istraga uistinu dovršena i obavljena na pravilan način. Navedeni zapisnici i dokumentacija istražitelja mogu sadržavati sljedeće informacije, [35]:

- datum i vrijeme početka istrage
- fizičko stanje uređaja
- fotografije uređaja koji je predmet istrage
- status uređaja - uključen ili isključen
- proizvođač uređaja i model
- alati korišteni za ekstrakciju i analizu
- podaci pronađeni tijekom istrage
- bilješke stručnog mišljenja.

Faza prezentacije

Tijekom istrage važno je osigurati da se ekstrahirani podaci i dokumentacija, sa svim informacijama o mobilnom terminalnom uređaju, mogu jasno predstaviti bilo kojim nadležnim osobama. Tijekom procesa forenzičke analize važno je kreirati forenzičko izvješće o ekstrahiranim podacima iz mobilnog terminalnog uređaja. To izvješće može uključivati podatke predstavljene u papirnatom i elektroničkom odnosno digitalnom obliku. Nalazi forenzičke istrage moraju biti dokumentirani i predstavljeni na način da dokazi govore sami za sebe kada se nalaze pred sudskim tijelima. Nalazi bi trebali biti jasni, sažeti i ponovljivi. Tako značajke, poput analize vremenske crte i komunikacijskih veza s drugim uređajima, koje nude mnogi komercijalni forenzički alati namijenjeni mobilnoj forenzici mogu pomoći u izvještavanju i objašnjavanju nalaza forenzičke istrage mobilnih terminalnih uređaja, [35].

Faza arhiviranja

Očuvanje i arhiviranje ekstrahiranih podataka iz mobilnog terminalnog uređaja važan je dio cjelokupnog procesa forenzičke analize. Također je važno da se podaci čuvaju u upotrebljivom formatu u svrhu provedbe sudskih postupka, za buduće potrebe ukoliko se dokazni materijal kompromitira ili ošteti te za potrebe čuvanja u svrhu evidencije. Određeni sudski predmeti mogu se odužiti kroz čitav niz godina prije donošenja konačne presude, a većina nadležnih sudskih tijela zahtijeva da se podaci

čuvaju kroz značajnije duže vremensko razdoblje u slučaju postupka žalbi na presude i dodatnih sudskih postupaka. Kako područje digitalne forenzike i metoda napreduju, nove metode ekstrakcije podataka biti će dostupne. Postoji mogućnost da će nove metode rezultirati nekim novim otkrićima u pogledu dokaza, a upravo će forenzički istražitelji to moći utvrditi na način da ponovo pregledaju stare podatke iz određenog slučaja izvlačenjem kopije dokaza iz arhive, [35].

3.4. Metode ekstrakcije

Forenzička akvizicija i analiza mobilnih terminalnih uređaja uključuje fizičke napore i upotrebu automatiziranih forenzičkih alata. Za obavljanje potreba mobilne forenzike postoji mnoštvo forenzičkih alata dostupnih na tržištu. Svaki od tih alata posjeduje svoje prednosti, ali i nedostatke te je bitno shvatiti da jedan korišten forenzički alat neće biti dostatan za obavljanje svih potreba tijekom procesa forenzičke analize. Kada se utvrde odgovarajući forenzički alati koji će se koristiti za akviziciju i analizu mobilnog terminalnog uređaja, potrebno je poznavati različite metode ekstrakcije podataka koje rezultiraju nejednakim količinama ekstrahiranih podataka i formatima datotekama koje je moguće pronaći na uređaju, [35]. Upravo je na slici 3 prikazana uobičajena klasifikacija metoda ili okvir koji služi za opisivanje načina kako se podaci ekstrahiraju iz mobilnih terminalnih uređaja.



Slika 3. Piramidalna struktura klasifikacije metoda ekstrakcije podataka
Izvor: [37]

Polazeći od dna piramide klasifikacije metoda i napredujući prema samome vrhu piramide, metode i forenzički alati postaju tehnički zahtjevniji, složeniji i invazivniji, ali su „forenzički prihvatljivi ili zvučni“ iako zahtijevaju duže razdoblje za provedbu analize pa tako postoje određene prednosti i nedostaci provođenja analize sa svakim slojem piramide na koje forenzički istražitelj treba obratiti pažnju. U slučaju da se predviđene

metode ili alati ne koriste na pravilan način, to može uzrokovati potpuno uništenje digitalnih dokaza s uređaja, a taj se rizik povećava polazeći prema vrhu piramide. Stoga je za provođenje zahtjevnijih metoda od ključnog značaja potrebno educirano i kvalificirano osoblje te odgovarajuća obuka kako bi se postigao uspjeh u ekstrakciji podataka s mobilnog terminalnog uređaja. Tako će svaka metoda imati različite implikacije i stope uspješnosti provedbe što će ovisiti o uporabljenom forenzičkom alatu, korištenoj metodi te modelu uređaja, [35], [37].

Prethodno prikazanu piramidu također je moguće podijeliti u dvije glavne kategorije metoda ekstrakcije, koje predstavljaju forenzičke metode kroz logičku ili fizičku prirodu. Logička metoda ekstrakcije izvlači i prikuplja alocirane ili dodijeljene podatke i to se obično ostvaruje pristupom datotečnom sustavu uređaja. Alocirani ili dodijeljeni podaci u jednostavnom značenju predstavljaju podatke koji se ne brišu u uređaju i dostupni su unutar datotečnog sustava uređaja. Jedna iznimka koja odstupa od prethodne definicije je da određene datoteke, kao što su neke baze podataka, mogu biti predstavljene kao alocirani podaci i sadržavati izbrisane zapise u pojedinoj bazi podataka. Iako oporavak izbrisanih podataka zahtijeva posebne forenzičke alate, tehnike i metode, moguće je do tih izbrisanih podataka doći i putem logičke metode. Logičke metode se često izvode kao prva vrsta istraživanja kojom će se služiti forenzički istražitelj. Pri korištenju takvih metoda nisu potrebni dodatni hardverski uređaji ili softverski programi. S druge strane, fizičke metode izravno ciljaju fizički medij za pohranu podataka i ne oslanjaju se na datotečni sustav uređaja kako bi se dobio pristup podacima. Najznačajnija prednost pristupa putem fizičkih metoda je u tome da će se vrlo vjerojatno omogućiti pristup značajnijoj količini izbrisanih podataka. Razlog tomu je da datotečni sustav podatke označava izbrisanim, ali ih ne trajno ne izbriše s medija za pohranu. Upravo kako fizičke forenzičke metode pružaju izravan pristup mediju za pohranu, moguće je oporaviti alocirane i izbrisane podatke, ali je takva metoda daleko teža i zahtjevnija, [35], [38].

3.4.1. Metoda ručne ekstrakcije

Ručna ekstrakcija predstavlja najjednostavniju metodu ekstrakcije podataka mobilnih terminalnih uređaja. Postupak je relativno brz i funkcionirat će na gotovo svakome mobilnom uređaju, osim ako u suprotnome uređaj nije zaključan. Ova metoda uključuje forenzičkog istražitelja koji korištenjem korisničkog sučelja mobilnog uređaja i manipulacijom fizičkih komponenti pristupa pregledu sadržaja koji je pohranjen na uređaju. Istraživač će pregledavati sadržaj na uređaju pristupajući različitim izbornicima i opcijama poput popisa poziva, tekstualnih poruka, IM (engl. *Instant Messaging*) platformi za slanje poruka kao što je *WhatsApp* i sl., dok na ovoj razini nije moguće vratiti izbrisane i prikupiti sve podatke.

Otkrivene informacije tj. trenutni prikaz zaslona uređaja moguće je dokumentirati putem fotografiranja pomoću digitalne kamere drugog uređaja i moguće ga je predstaviti kao dokaz. Pri korištenju ove metode potrebno je biti oprezan jer postoji velika sklonost ljudskim pogreškama. Takve pogreške mogu se dogoditi u slučaju

nedovoljnog poznavanja sučelja uređaja kojeg je potrebno istražiti ili prilikom pritiskanja pogrešnog gumba na zaslonu ili tipkovnici te tako izbrisati ili dodati podatke. Također, moguće je da će uređaj biti postavljen na stranom jeziku koji nije poznat istražitelju ili da je uređaj fizički oštećen ili neispravan pa da pojedine funkcije ili naredbe neće biti registrirane od strane uređaja, što će onemogućiti daljnji tijek istrage. Ručna ekstrakcija trebala bi se koristiti kao krajnje sredstvo za provjeru rezultata ekstrakcije tj. za verifikaciju podataka ekstrahiranih nekom od drugih metoda, [35], [37].

3.4.2. Metoda logičke ekstrakcije

U digitalnoj forenzici izraz logičke ekstrakcije obično se upotrebljava za označavanje ekstrakcija koje ne obnavljaju izbrisane podatke ili ne uključuju potpunu bit-po-bit kopiju podataka s uređaja. Međutim, ispravnija definicija logičke ekstrakcije predstavlja ju kao svaku metodu ekstrakcije koja zahtijeva komunikaciju s operativnim sustavom uređaja. Zbog te interakcije s operativnim sustavom uređaja, forenzički istražitelji ne mogu biti sigurni da su obnovili sve moguće podatke kako operativni sustav selektivno odabire kojim podacima će omogućiti pristup. U tradicionalnoj računalnoj forenzici logička ekstrakcija analogna je postupku kopiranja i lijepljenju te iste mape radi ekstrakcije podataka iz sustava. Tijekom tog postupka kopirati će se samo datoteke kojima korisnik može pristupiti i vidjeti ih. U slučaju da se u kopiranoj mapi nalaze skrivene ili izbrisane datoteke, one se neće nalaziti u novoj zalijepljenoj verziji mape. Tako se logička ekstrakcija može definirati i kao postupak koji ekstrahira podatke vidljive korisniku i može uključivati podatke koje je moguće označiti za brisanje, [39].

Metoda logičke ekstrakcije uključuje povezivanje mobilnog uređaja s dodatnim forenzičkim hardverom ili spajanje na forenzičku radnu stanicu putem USB kabela, RJ-45 (engl. *Registered Jack 45*) kabela ili *Bluetooth* tehnologije. Drugim riječima, vrši se sinkronizacija podataka koji se nalaze na mobilnom uređaju sa spojenim računalom. Jednom kada je uređaj povezan, računalo pokreće naredbe i prosljeđuje ih na uređaj te se kreirane naredbe na uređaju tumače od strane procesora. Zatim se traženi podaci, koji su predani putem naredbe, dohvaćaju iz memorije samoga uređaja i vraćaju natrag na forenzičku radnu stanicu koju će forenzički istražitelj kasnije biti u mogućnosti pregledati. Velika većina dostupnih forenzičkog alata djeluje na ovoj razini klasifikacijskog sustava metoda, [35], [37].

Pri ekstrakciji podataka ovom metodom forenzički alati komuniciraju s operativnim sustavom mobilnog uređaja pomoću API-ja¹² (engl. *Application Programming Interface*) koji određuje kako pojedine softverske komponente međusobno funkcioniraju. Forenzički alati koriste navedene API-je za komunikaciju s operativnim sustavom mobilnog uređaja i zahtijevanje pristupa podacima iz sustava. Logička ekstrakcija provodi se, većim dijelom, putem određenog API-ja dostupnog od strane dobavljača uređaja. Kao što API omogućuje komercijalnim aplikacijama treće strane da komuniciraju s operativnim sustavom, tako omogućavaju i forenzičku ekstrakciju

¹² API - aplikacijsko programsko sučelje, sučelje za programiranje aplikacija

podataka. Tipični podaci dostupni putem logičke ekstrakcije su popisi poziva, tekstualne poruke SMS (engl. *Short Message Service*), multimedijске poruke MMS (engl. *Multimedia Messaging Service*) poruke, fotografije, videozapisi, audio datoteke, kontakti, kalendari i podaci o aplikacijama, [40], [41].

Prednosti postupka ekstrakcije na ovoj razini odnose se na relativnu brzinu postupka tj. ne oduzima puno vremena, iznimno je jednostavna za uporabu, na raspolaganju će biti veća količina podataka naspram ručne ekstrakcije, podrška stranih jezika, a postupak je ponovljiv. S druge strane, tijekom provođenja postupka moguće je da će se određeni podaci upisati u mobilni uređaj što može promijeniti integritet digitalnih dokaza. Isto tako, izbrisani podaci s uređaja neće se prikupljati jer metoda pristupa samo alociranim podacima koji se nalaze unutar datotečnog sustava, a kao još jedna mana u odnosu na ručnu ekstrakciju navodi se velik broj potrebnih konekcijskih kablova zbog raznolikosti mobilnih uređaja, [35], [37].

3.4.3. Metoda fizičke ekstrakcije i JTAG metoda

Hex dump, koji se naziva i fizičkom ekstrakcijom, postiže se povezivanjem uređaja s forenzičkom radnom stanicom i prijenosom nepotpisanog koda ili *bootloadera*¹³ na mobilni uređaj koji će kasnije navoditi uređaj da prenese sadržaj svoje memorije na forenzičku radnu stanicu ili računalo. U digitalnoj forenzici, metoda fizičke ekstrakcija predstavlja preciznu bit-po-bit kopiju memorije uređaja i ekstrakciju pa je tako primjenjiva i za mobilne uređaje te uključuje izbrisane podatke po čemu se razlikuje od metoda logičke ekstrakcije. Ekstrakcija podataka fizičkim metodama, koje se temelje na hardveru, uglavnom uključuje dvije metode: JTAG i *chip-off*. Te tehnike obično je teško implementirati te zahtijevaju veliku preciznost i iskustvo kako bi se mogle provesti na stvarnim uređajima tijekom forenzičke istrage.

Fizička ekstrakcija kod mobilne forenzike rezultatom je ista onoj kod fizičke ekstrakcije računala, ali metode pristupa ekstrakciji su nešto drugačije. Na primjer, ako se ne koriste JTAG ili *chip-off* metode, uređaj se u određenoj mjeri mora pokrenuti kako bi se moglo pristupiti podacima. Budući da je rezultat dobivena sirova ili neobrađena slika u binarnom formatu, potrebna je tehnička stručnost kako bi se ona dodatno analizirala. Metoda pruža veću količinu ekstrahiranih podataka za analizu i omogućuje oporavak izbrisanih podataka na većini uređaja. Iako je kao sama metoda fizičke ekstrakcije najopsežnija, s druge strane je i najmanje podržana metoda ekstrakcije. Razlog najmanje podržanosti fizičke ekstrakcije leži u tome jer zahtjeva puni pristup unutarnjoj memoriji mobilnog uređaja koji u potpunosti ovisi o operativnom sustavu i sigurnosnim mjerama koje proizvođači uređaja koriste.

Koje je podatke moguće ekstrahirati ovom metodom? Ova metoda ekstrakcije omogućuje prikupljanje svih živih podataka, kao i podataka koji su izbrisani ili skriveni, što znači gotovo sve podatke, ali ne u svim slučajevima. Općenito govoreći, to je zbog nedostatka određenih forenzičkih alata ili u slučaju kada se podaci aplikacija kodiraju

¹³ *Bootloader* - program zadužen za pokretanje operativnog sustava

ili je uređaj zaključan. Ekstrakcijom bit-po-bit, kao što je ova, izbrisani podaci potencijalno mogu biti otkriveni. To znači da se podaci koji se nalaze izvan aktivnih korisničkih podataka i datoteka baza podataka, kao što su: fotografije, videozapisi, instalirane aplikacije, informacije o lokaciji i još mnogo toga može ekstrahirati dok se izbrisane podaci navedenih stavki mogu obnoviti, [35], [39], [40].

JTAG (engl. *Joint Test Action Group*) predstavlja udrugu koju je utemeljila elektronička industrija za razvoj metode provjere dizajna i testiranje matičnih ploča nakon proizvodnje. Primijenjeno u forenzičkom kontekstu, metoda JTAG uključuje uporabu naprednih načina za prikupljanje podataka. Te metode obuhvaćaju povezivanje na standardne testne pristupne priključke ili TAP (engl. *Test Access Port*) na uređaju, što znači da JTAG obično zahtijeva rastavljanje uređaja, te naredbe upućene prema procesoru uređaja kako bi se omogućio prijenos podataka pohranjenih na povezanim memorijskim čipovima.

Pomoću ove metode moguće je dobiti cjelovitu fizičku sliku uređaja. Iako je JTAG metoda učinkovita u ekstrakciji podataka, trebaju je provoditi samo iskusni i kvalificirani forenzički istražitelji. Prije pokušaja provedbe JTAG metode forenzički istražitelji moraju imati potrebnu odgovarajuću obuku, jer uslijed nepravilnog rukovanja tokom provedbe ove metode može doći do trajnog oštećivanja uređaja pa je iznimno bitno da JTAG metoda ne bi trebala rezultirati gubitkom bilo kakvih funkcionalnosti uređaja. Svaka pogreška u spajanju priključaka ili primjeni drugog napona može u potpunosti oštetiti uređaj. Kada se metoda izvede i uređaj se ponovo sastavi, uređaj treba raditi bez problema. Iako je JTAG metoda efikasna, preporučuje se prvo isprobati ranije spomenute logičke tehnike jer su one puno jednostavne za provedbu i zahtijevaju manje napora, [35], [42], [43].

3.4.4. Chip-off metoda

Chip-off metoda, kao što ime sugerira, je tehnika kojom se memorijski čipovi fizički uklanjaju s matične ploče iz uređaja i ispituju kako bi se ekstrahirali podaci te je kao takva izrazito destruktivna metoda. Podatke je zatim moguće ekstrahirati s izdvojenog memorijskog čipa pomoću posebne programerske jedinice ili adaptera na koji se čip priključi. Pomoću ove metode podaci se izravno čitaju s memorijskog čipa te omogućavaju ispitivanje i analizu teško oštećenih mobilnih terminalnih uređaja ili njihovih pojedinih dijelova te kada je uređaj zaključan ili kada posebne opcije za pristup uređaju nisu omogućene. Također, podaci koji su ekstrahirani iz memorijskog čipa uređaja bit će u neobrađenom obliku te ih je potrebno raščlaniti, dekodirati i interpretirati.

Upotreba programerske jedinice ili adaptera određena je vrstom memorijskog čipa koji se nalazi unutar mobilnog terminalnog uređaja. Međutim, primjena ove tehnike zahtijeva ne samo stručnost, već i skupu opremu te pojedine forenzičke alate. Iako su dimenzije, što se tiče veličine memorijskih čipova, standardizirane, postoji mnoštvo različitih oblika te radi te činjenice forenzički laboratoriji moraju posjedovati velik skup

različitih adaptera koji su iznimno skupi, ali i prijeko potrebni za ovu metodu. Uz to što je cjelokupan proces i oprema skupa, potrebno je zasebno specijalno osposobljavanje forenzičkih istražitelja i poznavanje hardverske razine mobilnih uređaja jer su u procesu uključeni postupak odmašćivanja i zagrijavanja memorijskog čipa što je ključ za njegovo uspješno izdvajanje. Nepravilni postupci tako mogu oštetiti sami memorijski čip i učiniti sve podatke nedostupnima tj. podaci će biti uništeni.

Kao što je ranije spomenuto, ova metoda je destruktivne prirode pa je preporučljivo, kada god je to moguće tj. prije fizičkog odvajanja memorijskog čipa iz mobilnog uređaja, da se ostalim metodama ekstrakcije pokuša doći do bilo kakvih podataka, ako je prethodno obrađenim metodama to moguće izvesti. Tako nakon uklanjanja memorijskog čipa s mobilnog uređaja, korištenje ili ponovno korištenje istraživanog uređaja više neće biti moguće. Za razliku od primjene JTAG metode gdje se uređaj nakon ispitivanja može nastaviti normalno koristiti, *chip-off* metoda obično rezultira uništavanjem uređaja jer je iznimno teško ponovno priključiti memorijski čip u mobilni uređaj. No bitna razlika između JTAG i *chip-off* metode je u tome što se JTAG koristi s uređajima koji su operativni, ali nepristupačni pomoću standardnih alata, dok *chip-off* to odrađuje s uništenim ili zaključanim uređajima, [35], [43].

3.4.5. Micro Read metoda

Micro Read metoda uključuje fizički pregled mobilnog uređaja i tumačenje podataka koji su vidljivi na memorijskom čipu uređaja. Forenzički istražitelji koriste elektronički mikroskop visoke snage za prikaz stanja memorijskog čipa u kojem se trenutno nalazi te se zatim analiziraju i prevode binarni zapisi 0 i 1 kako bi se odredili nastali ASCII¹⁴ (engl. *American Standard Code for Information Interchange*) znakovi. Velika prednost ove metode je u tome što je sposobna za izdvajanje i provjeru svih podataka iz memorije uređaja te se dobiva najbolja slika tj. uvid u ono što se događa na uređaju.

Cijeli proces iznimno je dugotrajan (potrebno najviše vremena za provedbu u usporedbi s drugim metodama) i skup te zahtijeva veliko znanje i obučavanje o poznavanju hardverske građe mobilnih uređaja. Zbog ekstremnih tehničkih karakteristika koje su uključene u *Micro Read* metodu, ona će se pokušati provesti samo u slučajevima kada je u pitanju najveća razina ugroze poput nacionalne sigurnosti i to nakon što su iscrpljene sve ostale metode i mogućnosti ekstrakcije. Postupak *Micro Read* metode rijetko se izvodi i trenutno ne postoji dobar način i okvir za dokumentiranje cjelokupnog postupka te isto tako trenutno ne postoje dostupni komercijalni alati za izvođenje ove metode. Razlog manjem korištenju ove metode je taj što su se ranije navedene metode iznimno poboljšale i daju relativno zadovoljavajuće rezultate te su tako smanjile potrebu za njezinim izvođenjem, [35], [37].

¹⁴ ASCII kod - znakovni kod za prikaz znamenaka, simbola, slova i drugih znakova

3.4.6. Ostale metode

Metoda datotečne ekstrakcije

Metoda datotečne ekstrakcije predstavlja dio ili podskup metode logičke ekstrakcije u kojoj se koriste API metode u kombinaciji s drugim protokolima ovisno o operativnom sustavu uređaja. Tako se unutar ove metode koriste različite tehnike koje su specifične za svaki pojedini uređaj kako bi se omogućilo kopiranje datotečnog sustava. U nekim slučajevima ekstrakcije podataka potrebno se osloniti na sigurnosne kopije uređaja kako bi se omogućio pristup dostupnim i skrivenim datotekama te drugim podacima koji nisu nužno dostupni putem API-ja uređaja koji se koristi unutar metode logičke ekstrakcije. Količina ekstrahiranih podataka kojom rezultira ova metoda otprilike se može svrstati između metoda logičke i fizičke ekstrakcije. Karakteristika ove metode je da dohvaća sve pohranjene datoteke u memoriji uređaja koji se smatraju zauzetim tj. alociranim, dok u slučaju formatiranja memorije uređaja, s tom metodom neće se moći doći do bilo kakvih podataka. Unutar datoteka na uređaju moguće je pronaći neke naizgled nevidljive informacije poput obrisanih i privremenih sadržaja te ostataka tragova nekih prijašnjih datoteka te se dobiva pristup podacima i hijerarhiji u datotečnom sustavu uređaja poput *log* zapisa, sistemskih podataka, strukture podataka, povijesti pretraživanja i sl., [41].

Metoda ekstrakcija podataka putem sigurnosne kopije uređaja

U početku pojave raznih operativnih sustava povezanih s pametnim mobilnim terminalnim uređajima, nije postojao mehanizam koji bi korisniku omogućavao izradu sigurnosnih kopija vlastitih osobnih podataka. Kao rezultat toga, razvijene se i distribuirane razne aplikacije koje kreiraju sigurnosnu kopiju uređaja. Aplikacije napravljene u svrhu kreiranja kopije imale su mogućnost pohrane kopije na memorijsku karticu uređaja ili pohrane u oblaku. U svakom slučaju, korisnicima je omogućeno da mogu napraviti sigurnosnu kopiju svojih uređaja, a po potrebi i vratiti potrebne podatke s pohranjene kopije. Ovo ne predstavlja samo koristan način da se korisnik zaštiti od gubitka podataka, već može biti i izvrstan izvor podataka i informacija za potrebe forenzičke analize. Kasnije su se pojavile i nove opcije sigurnosnih kopija putem API-ja. Programeri bi jednostavnim putem mogli integrirati te API-je unutar svojih aplikacija, dok bi ostatkom sigurnosnih kopija upravljao operacijski sustav ili Google. Na taj način korisnici dobivaju sigurnosnu kopiju temeljenu na pohrani u oblaku s dosljednošću među aplikacijama. Bez obzira na koji način se vrši izrada sigurnosne kopije uređaja, forenzički istražitelji trebali bi utvrditi postoji li ona na uređaju te gdje je spremljena jer podaci pohranjeni unutar sigurnosne kopije mogu biti od velikog značaja u ispitivanju i provedbi forenzičke analize, [38].

ISP metoda

ISP (engl. *In-System Programming*) metoda predstavlja sličnu, ali nježniju verziju *chip-off* metode. Ova metoda za razliku od *chip-off* metode ne uključuje odmašćivanje memorijskog čipa s matične ploče mobilnog uređaja nego se umjesto toga koriste

vanjski vodiči, koji se povezuju na specifične točke memorijskog modula, pomoću kojih se kopiraju podaci memorijskog čipa. ISP metoda tako je usmjerena na uređaje koji sadrže eMMC (engl. *Embedded Multi Media Controller*) memorijske čipove koji integriraju *flash* memoriju i kontroler u jedan modul, [43].

3.5. Antiforenzika

Ako je forenzika primjena znanstvenog pristupa u zakonske svrhe kako bi se utvrdile činjenica u sudskim ili pravnim postupcima, tada je antiforenzika suprotna akcija. Antiforenzika, u koju pripadaju antiforenzički alati i tehnike, predstavlja značajan izazov prilikom provedbe forenzičke analize i kriminalističke istrage forenzičkim istražiteljima, ali i forenzičkim alatima. Za definiciju antiforenzike postoji širok izbor tumačenja. Od toga da antiforenzika predstavlja pokušaj ograničavanja identifikacije, prikupljanja, uspoređivanja i provjere valjanosti digitalnih podataka pa do svakog pokušaja ugrožavanja dostupnosti ili korisnosti dokaza tijekom procesa forenzičke analize. Sukladno tome, može se reći da je antiforenzika pokušaj negativnog utjecaja na postojanje, količinu i kvalitetu dokaza kako bi se otežali ili onemogućili pregledi i analize digitalnih dokaza s uređaja. Prvobitna namjena digitalne antiforenzike bila je skrivanje, promjena, zaštita i uništenje podataka tj. potencijalnih digitalnih dokaza te ometanje samog procesa digitalne forenzike napadom na forenzičke alate, [44].

Antiforenzika ima širok raspon područja primjene i svrhe. Ciljevi antiforezičkih metoda su sakriti, uništiti, zbuniti forenzičke istražitelje ili na bilo koji drugi način eliminirati izvor dokaza. Sakrivanje se odnosi na smještanje datoteka unutar drugih datoteka ili na onemogućavanje čitanja datoteka putem enkripcije. Uništavanje se odnosi na nepovratno brisanje ili prepisivanje sadržaja datoteka. Zbunjivanje je čin prepisivanja sadržaja datoteka pogrešnim podacima, dok se eliminacijom izvora mogu ukloniti potencijalni dokazi. Važno je napomenuti da bi neka metoda protiv forenzike mogla biti višenamjenska. Često postoji više načina za obavljanje određenih zadataka, pa isto vrijedi i za provedbu antiforenzike te se antiforenzičke metode razvrstavaju prema vektoru namjene. Iako postoje različita poimanja kategorizacije metoda protiv forenzike, postoje prividne sličnosti. Prema izvorima [44], [45] i [46] glavna podjela antiforenzičkih metoda svrstana je u sljedeće četiri kategorije:

- eliminacija dokaza
- sakrivanje dokaze
- uništavanje dokaza
- napadi na forenzičke alate.

Tijekom kriminalističke istrage i forenzičke analize, forenzički istražitelji pokušavaju steći digitalnu sliku analiziranog uređaja. Nekoliko je glavnih ciljeva forenzičkog postupka, a to su: pronalaženje dokaza, njihovo prikupljanje te očuvanje njihovog izvornog stanja. Naprotiv, cilj antiforenzike biti će upravo zaoblazanje tih postupaka. Jedan od najjednostavnijih načina borbe protiv eliminacije dokaza je blokiranje pristupa digitalnim uređajima koji se ispituju. To se primjerice može provesti kroz fizička

ograničenja pristupa korištenjem specijalnih brava i sefova. S druge strane, to mogu biti softverska ili hardverska ograničenja poput zabrane korištenja drugih mobilnih uređaja ili pristupa određenim aplikacijama ili uslugama. Alternativna antforenzička tehnika mogla bi biti neutralizacija izvora dokaza.

Ako se prvotnom metodom ne mogu eliminirati dokazi, iduća metoda bila bi sakrivanje dokaza. Ova metoda ne pokušava uništiti ili manipulirati dokazima već ih pokušava učiniti manje vidljivima tijekom procesa forenzičke istrage. U ovoj metodi, iznimno je bitno napomenuti da je sakrivanje dokaza gotovo jednako važno kao i alat koji se koristi za njihovo sakrivanje. U slučaju da forenzički istražitelji otkriju nazočnost alata za skrivanje podataka, samo to otkriće može predstavljati inkriminirajući dokaz. Uspjeh skrivanja dokaza ovisi o ljudskom faktoru i ne postoji garancija da će skrivanje dokaza biti potpuno uspješno. Kriptografija zapravo predstavlja jedan pristup koji omogućava djelomično sakrivanje podataka.

Uništavanje dokaza odnosi se na postupak da se dokazi učine neupotrebljivima tj. da se u potpunosti izbrišu svi podaci ili informacije s uređaja. Prilikom spomena brisanja podataka treba biti svjestan da se podaci stvarno ne mogu izbrisati, već postoje tehnike kojima se podaci prepisuju te u tu svrhu postoje softverski alati za prepisivanje cijele pohrane uređaja ili pojedinačnih datoteka. Prepisivanje cijele pohrane relativno je jednostavno s korištenjem određenih alata, ali problem predstavlja to što alat može ostaviti trag da je korišten u sustavu uređaja.

U napadima na forenzičke alate podrazumijevaju se napadi i pokušaji zavaravanja forenzičkih alata koje koriste forenzički istražitelji u forenzičkim istragama, tako da se sakriju aktivnosti, promjene određene sistemske vrijednosti na uređaju i sl. Jedan od načina je korištenje antforenzičkog alata koji briše sve tragove aktivnosti korisnika kako na uređaju i aplikativnim programima tako i na Internetu. Ovim se onemogućuje pronalaženje aktivnosti od strane forenzičkih istražitelja zaduženih za provedbu forenzičke istrage. Također, čest slučaj u praksi je i korištenje alata za promjenu datuma sustava i vremena kreiranja, modificiranja, pristupa i ažuriranja datoteka.

4. Forenzički programski alati usmjereni nosivim terminalnim uređajima

Nosivi terminalni uređaji kao mobilni uređaji i dio IoT okruženja spadaju u dinamičke sustave koji predstavljaju izazove iz forenzičke perspektive. Uz njihov napredak, globalno se razvijaju i novi modeli pametnih mobilnih uređaja koji zajedno s nosivim uređajima stvaraju zaokruženu komunikacijsku cjelinu. Sve veći broj i raznolikost mobilnih uređaja otežava razvoj jedinstvenog forenzičkog postupka ili alata za rješavanje svih potreba u procesu forenzičke analize. Pored toga, za ekstrakciju podataka s uređaja potrebna je interakcija sa sustavom uređaja, što često ima tendenciju mijenjanja njegovog stanja i može dovesti do uništenja ili promjene postojećih podataka na uređaju. Srećom, određenim forenzičkim metodama i tehnikama moguće je pribaviti digitalne dokaze s mobilnih uređaja na „forenzički prihvatljiv ili zvučan“ način, koji će kasnije biti pravovaljani u slučaju sudskih postupaka. Mobilni uređaji predstavljaju izazov i sa stajališta oporavka i analize sadržanih podataka. Međutim, glavna prednost mobilnih uređaja iz forenzičke perspektive je ta što mogu sadržavati izbrisane podatke čak i nakon što ih pojedinac pokuša kompromitirati, a upravo forenzički alati ovdje stupaju na scenu.

Uz prethodno spomenute uređaje, forenzički su alati također u stalnom razvoju. Nužno je to kako bi se osigurala prikladna sredstva za ekstrakciju podataka s različitih mobilnih uređaja putem nekih od ranije navedenih forenzičkih metoda. Svi forenzički alati po principu funkcioniraju na sličan način: šalju naredbe u mobilni uređaj te bilježe odgovore koji sadrže podatke pohranjene u memoriji uređaja. Podatke koje je moguće dobiti procesom ekstrakcije pomoću metoda ovise o mehanizmu veza i modelu samoga uređaja, [47].

4.1. Svrha i ograničenja forenzičkih alata

Postojeći forenzički alati u području digitalne forenzike ne mogu se adekvatno uklopiti u raznoliku infrastrukturu IoT okruženja u koju se svrstavaju i sami nosivi terminalni uređaji. Ogromna količina mogućih dokaza koji se generiraju velikim brojem IoT uređaja donose nove izazove u pogledu prikupljanja dokaza iz IoT infrastrukture. Osim toga, budući da zločinci ili treće osobe mogu utjecati na dokaze unutar IoT uređaja putem raznih mogućih metoda, poput udaljenog brisanja podataka, zbog slabe razine sigurnosti tih uređaja, ekstrakcija podataka tj. budućih dokaza možda neće biti prihvatljiva u okviru sudskih postupaka. Stoga je potrebno riješiti sve trenutno poznate izazove te pronaći metodu za prevladavanje prepreka i osmisliti nove alate za provedbu forenzičke istrage IoT-a, koja će biti odobrena od strane sudskih tijela i kojom će se postići ciljevi forenzičkih istražitelja, [32].

Iskustva u manipulaciji računalima pomoću zlonamjernih programa ili drugih tehnika, koja su se kasnije pojavila na mobilnim terminalnim uređajima, a danas i na IoT uređajima, sugeriraju da svugdje gdje postoje mogućnosti tehničke eksploatacije

postoji i vjerojatnost kibernetičkih napada. Zato se predviđa porast broja napada na IoT okolinu. To mobilizira stručnjake za informatičku i kibernetičku sigurnost te forenzičke stručnjake kako bi bili spremni reagirati na nadolazeće prijetnje. Iako je znano da je prevencija bolja od liječenja, napade nije moguće u potpunosti ukloniti, ali se mogu značajno ublažiti. Pravodobna reakcija na incident i forenzička analiza zločina ili napada jednako su važni i potrebni kao osiguranje cjelokupne komunikacijske mreže, [31].

Forenzički alati za digitalnu forenziku namijenjeni su pružanju potpore nadležnim službenim tijelima za provedbu zakona i forenzičkim istražiteljima u prepoznavanju, prikupljanju, očuvanju i analizi podataka mobilnih uređaja za koja se pretpostavlja da su povezana s neprimjerenim i nezakonitim radnjama koje uključuju kibernetički kriminal, razne kriminalnih aktivnosti te slične povezane postupke. Forenzički alati često se miješaju s drugim klasifikacijama alata, kao što su alati za upravljanje incidentima i oporavak podataka. No iako se oni mogu koristiti i u te svrhe, razlika je u tome što je prilikom upotrebe forenzičkih alata potrebno pridržavanje formalnih protokola tijekom obrade uređaja i distribucije dokaza te izbjegavanje bilo kakve izmjene ili kompromitacije podataka, omogućujući da se finalni produkt forenzičke analize može uspješno koristiti u sudskim procesima, [48].

Alati za digitalnu forenziku predstavljeni su kroz hardverske i softverske alate koji se mogu upotrijebiti za oporavak i očuvanje digitalnih dokaza. Većina takvih dostupnih proizvoda, bilo da se radi o komercijalnim alatima ili alatima otvorenog koda (engl. *open source*), koncentrirana je na računalnu forenziku i forenziku mobilnih uređaja, upravo radi toga jer su to dvije prevladavajuće grane forenzike. Hardverski alati osmišljeni su prije svega za ispitivanje svih uređaja s mogućnošću pohrane podataka, a cilj im je da uređaji, koji su dokazni materijal, ostanu nepromijenjeni kako bi se očuvala cjelovitost podataka i dokaza. Takav alat predstavlja forenzički diskovni kontroler ili hardverski blokator uređaja koji služi samo za čitanje podataka te tako forenzičkim istražiteljima omogućuje pregledavanje zapisanih podataka na uređaja bez opasnosti od izmjene ili brisanja sadržaja. Većina je forenzičkih softverskih alata višenamjenska i mogu obavljati različite zadatke unutar jedne aplikacije. Neke od tih aplikacija otvorenog su koda, što iskusnim forenzičkim istražiteljima omogućuje izmjenu koda u skladu s njihovim specifičnim potrebama u procesu forenzičke analize te osiguravaju financijsku uštedu kako se ne bi morali koristiti drugi alati. Neki softverski alati tako mogu istovremeno obrađivati više uređaja ili upravljati različitim operativnim sustavima. Mogućnosti ovih aplikacija kategoriziraju se po granama digitalne forenzike u kojima se koriste. Dok se hardverski alati poput blokatora uređaja prvenstveno fokusiraju na očuvanje podataka unutar uređaja, softverske aplikacije su ih u mogućnosti ekstrahirati i analizirati čime značajno pomažu u efikasnosti tijekom procesa forenzičke analize.

Osumnjičene osobe često sakrivaju ili brišu svoje podatke na uređajima kako bi se teško otkrili kompromitirajući dokazi unutar memorije uređaja. Međutim, forenzički alati mogu pomoći istražiteljima u obnavljanju tih dokaza na taj način da se određene

korisničke aktivnosti mogu oporaviti i istražiti pojedinim softverskim alatima za digitalnu forenziku. U slučajevima forenzike mobilnih uređaja, većina digitalnih uređaja s unutarnjom memorijom i komunikacijskom sposobnošću, poput GPS uređaja ili pametnih satova, može se istražiti pomoću ovih aplikacija. Aplikacijama je prvenstven fokus na aktivnostima osumnjičenih osoba na mobilnom uređaju. Na primjer, aplikacije unutar uređaja mogu se analizirati na način da se utvrdi kada je i kako s mobilnog terminalnog uređaja odaslan određen podatak. Popise telefonskih poziva moguće je oporaviti radi provjere alibija osumnjičene osobe ili uspostavljanja vremenskih tijekova određenih događaja, dok se tekstualne poruke poslone putem SMS-a ili *WhatsApp* aplikacije mogu pretraživati prema ključnim riječima kako bi se olakšali postupci analize. Forenzički istražitelji također mogu oporaviti GPS lokaciju s mobilnog uređaja ili iz usluga temeljenih na lokaciji kako bi se dobio zapis o kretanju mobilnog uređaja, [49].

Za potrebe ekstrakcije podataka, logički sustavi ostvaruju interakciju te komuniciraju s operativnim sustavom mobilnog uređaja kako bi izvukli pojedine podatke. Uz takvo funkcioniranje logičkih sustava postoje određena ograničenja prilikom ekstrakcije podataka te su u tim slučajevima dostupne samo informacije vezane uz operativni sustav uređaja. Tako se potencijalno relevantni podaci vezani za forenzičku istragu možda neće uspjeti ekstrahirati, dok se izbrisane stavke uopće neće niti pokušavati ekstrahirati. Primjerice, pametni mobilni terminalni uređaji sadrže sljedeće podatke koje je gotovo uvijek moguće ekstrahirati: popis kontakata, popisi poziva, SMS poruke i fotografije, dok dodatne informacije nisu garantirane, [47].

Trenutno na tržištu postoji nekoliko komercijalnih forenzičkih alata, koji se prezentiraju kao posebno dizajnirani alati za ekstrakciju i prikupljanje podataka s pametnih mobilnih terminalnih uređaja i pojedinih aplikacija te pripadajućih nosivih terminalnih uređaja. U svrhu izrade diplomskog rada te da bi potkrijepili te navode bili su testirani sljedeći alati:

- *Belkasoft Evidence Center*
- *Magnet Axion Process*
- *Oxygen Forensic Detective*
- *SPF Pro*.

Od nekoliko spomenutih alata samo se jedan pokazao kao djelotvoran u području digitalne forenzike nosivih terminalnih uređaja, a to je *Oxygen Forensic Detective*. Ostali alati ne pružaju potporu forenzičkoj analizi korištenih mobilnih nosivih uređaja i aplikacija. Zbog toga će za potrebe ovoga diplomskog rada u idućim poglavljima biti obrađivan forenzički alat *Oxygen Forensic Detective*, koji je zadovoljio tražene kriterije.

4.2. Oxygen Forensic Detective

Softverska tvrtka PC-to-Mobile Communication osnovana je 2000. godine, a kasnije je preimenovana u Oxygen Forensics. Iskustvo i znanje stečeno u razvoju aplikacija u prvom razdoblju rada tvrtke, dalo je izvrsnu podlogu za razumijevanje komunikacijskih protokola mobilnih uređaja. Upravo ti temelji dali su poticaj za ugrađivanje inovativnih tehnika u forenzički alat *Oxygen Forensic Detective*. Pojavom navedenog alata na tržištu, korisnicima je omogućen pristup mnogo kritičnijim podacima i informacijama nego što su u to vrijeme pružali konkurentski forenzički alati za forenzičku analizu. Danas je to jedan od iznimno bitnih alata zato što omogućuje forenzička ispitivanje raznolikih vrsta uređaja poput pametnih mobilnih terminalnih uređaja, IoT uređaja, nosivih terminalnih uređaja (pametnih satova) te bespilotnih letjelica tj. dronova. Jedna od iznimnih prednosti ovoga alata je ta što se njime dobiva univerzalno forenzičko rješenje koje pokriva najširi raspon mobilnih terminalnih uređaja, [50].

Oxygen Forensic Detective napredno je forenzičko softversko rješenje dizajnirano za ekstrakciju i analizu podataka s mobilnih uređaja, njihovih sigurnosnih kopija i slika te memorijskih čipova. Softver pruža logičku podršku najširem rasponu mobilnih uređaja i omogućuje potpuno automatizirano forenzičko prikupljanje i analizu te je do danas odigrao značajnu ulogu u raznim kriminalnim i drugim istragama diljem svijeta. Prema [51] s alatom *Oxygen Forensic Detective* moguće je:

- ekstrahirati sve podatke o mobilnom uređaju, koji uključuju: kontakte, pozive, poruke, datotečni sustav, lozinke, GPS lokacije, izbrisane podatke i podatke iz svih popularnih aplikacija
- dohvatiti podatke sa SIM i memorijskih kartica
- ekstrahirati podatke iz pametnih satova temeljenih na *MediaTek* čipovima
- ostvariti pristup podacima iz 62 različita izvora pohrane u oblaku uključujući iCloud, Google, Microsoft, Huawei, Samsung, Mi Cloud, FitBit itd.
- ekstrahirati podatke s IoT uređaja poput *Amazon Alexa* i *Google Home*
- dohvatiti povijest letenja s pripadajućim metapodacima, fotografijama i videozapisima s bespilotnih letjelica tj. dronova te ekstrahirati podatke mobilnih aplikacija povezanih s dronovima
- analizirati ekstrahirane podatke u ugrađenim analitičkim odjeljcima, poput vremenske trake (engl. *Timeline*), društvenog grafikona (engl. *Social Graph*), ključnih dokaza (engl. *Key Evidence*) te agregiranih kontakata (engl. *Aggregated Contacts*)
- pretraživati podatke koristeći različite metode koje uključuju regularne izraze, popise ključnih riječi itd.
- napraviti izvješća o dokazima u različitim formatima datoteka.

Trenutna verzija ovoga alata podržava 26.000+ mobilnih uređaja koje pokreću različite vrste operativnih sustava. *Oxygen Forensic Detective* omogućava uvoz i analizu podataka iz različitih sigurnosnih kopija i slika uređaja koje su napravljene putem drugih forenzičkih alata, [51].

Nosivi terminalni uređaji i aplikacije za praćenje zdravlja mogu bilježiti razne podatke poput otkucaja srca, razdoblja spavanja, lokaciju i još mnogo toga. Što je još važnije, upravo su podaci s ovih uređaja bili ključni u rješavanju nekoliko važnih kriminalističkih istraga. U svakoj novoj, ažuriranoj verziji *Oxygen Forensic Detectivea* mogućnosti ekstrakcije se dodatno proširuju i obuhvaćaju sve veće područje u kojima je moguće provesti forenzičku analizu. Tako je uz porast popularnosti pametnih satova u novijim inačicama forenzičkog alata dodana mogućnost ekstrakcije podataka iz pametnih satova koji se temelje na setovima *MediaTek* čipova. Moguće je izvršiti logičku akviziciju tih pametnih satova što će omogućiti forenzičkim istražiteljima da izdvoje podatke poput modela uređaja, kontakte, pozive, poruke, multimedijske datoteke i druge podatke. Upravo takvim naporima od strane tvrtke Oxygen Forensics došlo se do razine ekstrakcije podataka iz zdravstvenih aplikacija poput *Fitbit*, *Google Fit*, *Samsung Health* i sl., [52], [53].

Što se tiče pojedinih opcija unutar forenzičkog alata, potrebno je istaknuti neke od njih. Odjeljak vremenske trake nudi kronološki pregled svih događaja na uređaju - poruke, razgovori unutar aplikacija, pozivi, web aktivnosti, povezivanja na Wi-Fi, fotografije s vremenskim oznakama te još mnogo toga. Događaji se mogu pregledavati samostalno za jedan uređaj ili za grupu uređaja čime se omogućuje lako prepoznavanje uobičajenih grupnih aktivnosti ako su uređaji na bilo koji način bili međusobno u komunikaciji. Unutar ovog odjeljka tražene podatke moguće je pregledavati, poredati i filtrirati prema datumu, vremenu, učestalosti aktivnosti, kontaktima ili drugim podatkovnim točkama koje su potrebne za provedbu određene forenzičke analize. Također, postoji i opcija vizualizacije svih lokacija putem satelitske mape te kreiranja ruta na temelju pojedinih geografskih točaka koje mogu biti generirane na temelju aktivnosti određenih aplikacija, metapodataka s fotografija i veza temeljenih na lokaciji, [54].

5. Postupak i elementi forenzičke analize nosivih uređaja

Iako u području mobilne forenzike i forenzike aplikacija postoji znatan broj radova koji opisuju postupke i iznose rezultate procesa forenzičke analize, mali je broj radova koji se konkretno odnose na nosive terminalne uređaje. Upravo se radi toga diplomski rad bazira na nosivim terminalnim uređajima zbog postojanja potencijala u otkrivanju novih mogućnosti procesa forenzičke analize i ekstrahiranih podataka.

U radu i istraživanju *Watch What You Wear: Preliminary Forensic Analysis of Smart Watches* izdanom od strane autora Baggili, J., Oduro, J., Anthony, K., Breitingner, K., McGee, G., predstavljena je preliminarna forenzička analiza dvaju popularnih modela pametnih satova i pametnog mobilnog terminalnog uređaja koji su međusobno bili sinkronizirani. Istraživanje se oslanja i opravdava na budućnosti prihvaćanja korištenja nosivih terminalnih uređaja od strane korisnika čime se dolazi do pokazatelja korisnosti forenzičke analize samih uređaja, [55].

Nosiva tehnologija postaje sve veća stavka u području mobilne forenzike pa su tako pametne naočale *Google Glass* pretežito prilagođene i posvećene funkcijama društvenih mreža. Upravo takvom karakterističnom prilagodbom efekt takvih funkcija predstavljen je kroz slučaj generiranja velike količine podataka koji su pogodni i interesantni za forenzička istraživanja kako se navodi u radu Geradts, Z.: *Extraction and Forensic Analysis of Artifacts on Wearables*, [56].

Upravo su inovacije u području pametnih mobilnih uređaja dovele do toga da se ti uređaji koriste više od bilo kojeg drugog uređaja u svakodnevnom životu. *Android* pametni sat pripada jednim od popularnijih uređaja koji se koriste u svijetu, iako je samo moguća njegova interakcija s *Android* temeljenim operacijskim sustavima. Pametni sat može sadržavati puno korisnih informacija o korisniku uređaja, a one su kao takve pohranjene u uređaju i procesom forenzičke analize moguće im je pristupiti i odrediti slijed određenih događaja. Upravo rad autora Parikh, S., Chavda, D., Chakraborty, S., Rughani, P., Dahiya, M. S.: *Analysis of Android Smart Watch Artifacts* raspravlja o tome koje su sve informacije dostupne na *Android* pametnom satu i analizira njihovu korisnost u pogledu cjelokupne forenzičke analize, [31].

Nadalje, kada se govori o popularnim zdravstvenim ili sportskim aplikacijama te koje podatke zapravo one pohranjuju najbolje je obrađeno u radu *Android Nike Run app - Geolocation, SQLite views & self joins*, autora Brignoni, A. S ovim radom dobiva se cjelokupna pozadinska slika o aplikacijama i njihovoj pravoj vrijednosti, a to su korisnički podaci kojima je moguće pristupiti forenzičkom analizom, [57].

Tako su prethodno navedeni radovi postali temeljna okosnica izrade ovoga diplomskog rada da zatim bi u vlastitom pokušaju forenzičkog istraživanja pokušali identificirati potencijalne forenzičke vrijednosti. U nastojanju dobivanja takvih rezultata potrebno je obraditi uređaje i ekstrahirati podatke kojima je moguće pristupiti putem pametnog sata ili pametnog mobilnog terminalnog uređaja. S tim ciljem, testirana su

dva reprezentativna mobilna uređaja, nosivi terminalni uređaj tj. pametni sat te pripadajući povezani pametni mobilni terminalni uređaj.

Korištena oprema

Za potrebe provedbe forenzičkog istraživanja bilo je potrebno sljedeće:

- Pametni mobilni terminalni uređaj - *Samsung Galaxy A8*
- Nosivi terminalni uređaj, pametni sat - *Samsung SM-R380 Gear 2*
- Zdravstvena fitness aplikacija - *Runkeeper GPS Track Run Walk*
- Forenzički alat - *Oxygen Forensic Detective*

Operativni sustavi uređaja te inačice aplikacija i alata, koje su bile u uporabi u trenutku provođenja procesa forenzičke analize, bile su ažurirane na posljednje nadogradnje koje su omogućene od strane proizvođača:

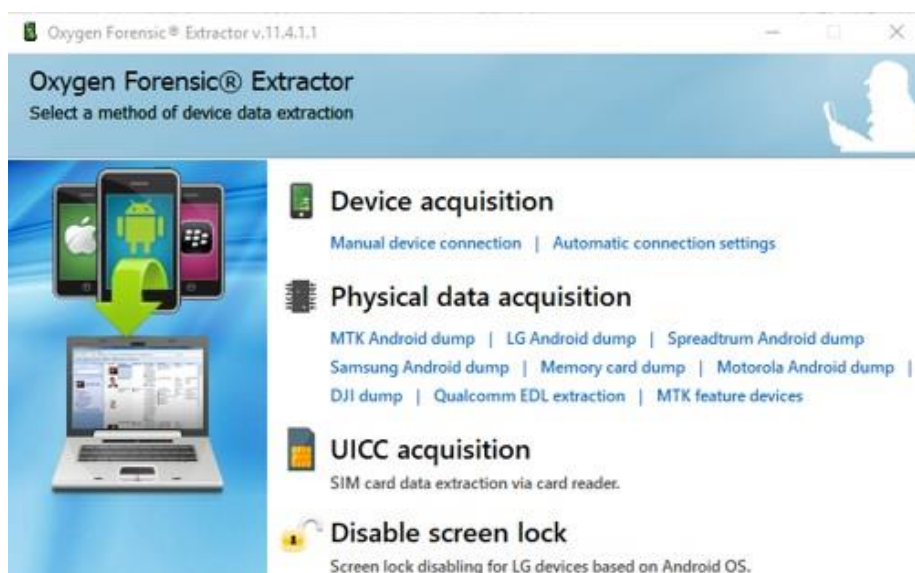
- *Samsung Galaxy A8* - operativni sustav *Android 9.0* poznatiji pod nazivom *Android Pie*
- *Samsung SM-R380 Gear 2* - operativni sustav *Tizen 2.2.1.2*
- *Runkeeper GPS Track Run Walk* - verzija 9.9.1
- *Oxygen Forensic Detective* - verzija 11.4.1.1

Pametni mobilni terminalni uređaj *Samsung Galaxy A8* prvotno je povezan putem *Bluetooth* tehnologije s pametnim satom da bi se zatim instalirala zdravstvena fitness aplikacija *Runkeeper*. Uređaji i aplikacija s namjerom su bili korišteni u svakodnevnom životu kako bi se prikupila dovoljna količina podataka te da se dobije uvid u maksimalne mogućnosti procesa forenzičke analize. Također, važno je napomenuti da prilikom provođenja procesa forenzičke analize na uređajima nisu bile korištene nikakve dodatne opcije pristupa osim što je uključen programerski način rada na uređaju kako bi se omogućilo otklanjanje pogrešaka putem USB-a.

Nakon određenog razdoblja testiranja uređaja i aplikacije, te kada se pretpostavilo da su zadovoljeni određeni kriteriji prikupljene količine podataka, bilo je moguće pristupiti procesu forenzičke analize svih uređaja. Postupci forenzičke analize prikazani su u nastavku.

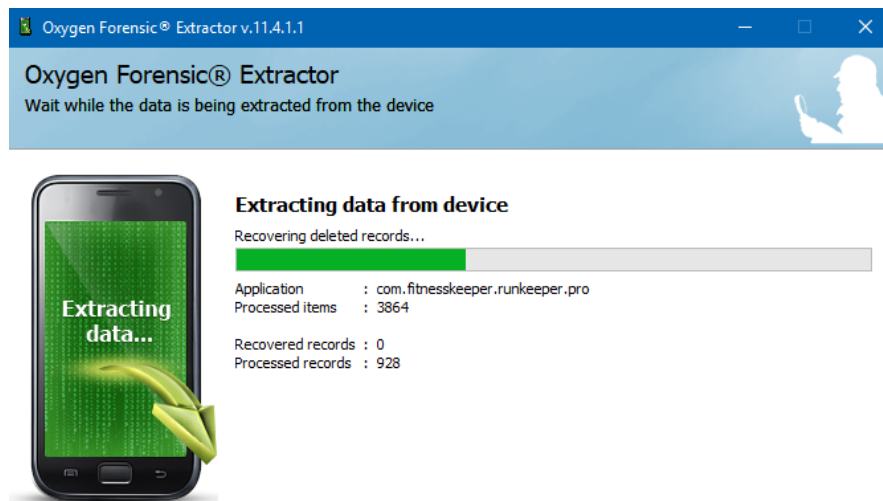
5.1. Forenzička analiza pametnog mobilnog terminalnog uređaja

Na početku postupka forenzičke analize prvo je potrebno otvoriti forenzički alat, u ovome slučaju *Oxygen Forensic Detective* te putem USB kabela spojiti pametni mobilni terminalni uređaj, *Samsung Galaxy A8*, kako bi uređaj bio prepoznat te da bi se otvorio unutar forenzičkog alata za potrebe provedbe ekstrakcije podataka. Nakon što je uređaj prepoznat u forenzičkom alatu, otvaraju se sve opcije koje je moguće provesti s povezanim uređajem, što je prikazano na slici 4.



Slika 4. Sučelje forenzičkog alata *Oxygen Forensic Detective* nakon prepoznavanja pametnog mobilnog terminalnog uređaja

Prilikom provedbe forenzičke analize nad uređajima, testirane su bile sve moguće opcije koje su prikazane na prethodnoj slici, no kao najbolja opcija pokazala se metoda *Device acquisition* koja nudi dvije varijante: zadani način rada (engl. *Default mode*) te napredni način rada (engl. *Advanced mode*) u kojem je moguće odabrati dodane opcije poput metode fizičke ekstrakcije ili metode ekstrakcije putem sigurnosne kopije uređaja, na koje će se osvrnuti u idućem poglavlju. Nakon odabranog načina ekstrakcije pristupa se samomu procesu ekstrakcije podataka s uređaja, kako je prikazano na slici 5.



Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.

Slika 5. Postupak provođenja ekstrakcije podataka s pametnog mobilnog terminalnog uređaja

Nakon završetka procesa ekstrakcije podataka, otvara se novi prozor unutar forenzičkog alata, slika 6, koji obavještava forenzičkog istražitelja da je proces završen te navodi pojedine korake obuhvaćene opcijom ekstrakcije te jesu li uspješno izvršeni ili nisu. Također nudi se i opcija pregleda i analize ekstrahiranih podataka, kao i spremanje ekstrahiranog uređaja u arhivu te izvoz i opcija ispisa cjelokupnog izvješća.



Slika 6. Ishod procesa ekstrakcije podataka pametnog mobilnog terminalnog uređaja

5.2. Forenzička analiza nosivog terminalnog uređaja

Postupak provođenja ekstrakcije podataka s nosivog terminalnog uređaja u ovome slučaju pametnog sata Samsung, predstavljen je kroz slične korake kao i sama ekstrakcija podataka sa pametnog mobilnog terminalnog uređaja koja je prethodno navedena.

U početku procesa postupka forenzičke analize potrebno je otvoriti forenzički alat, također u ovome slučaju *Oxygen Forensic Detective* te putem USB kabela povezati nosivi terminalni uređaj, pametni sat *Samsung SM-R380 Gear 2*, kako bi uređaj bio prepoznat unutar forenzičkog alata radi daljnje svrhe provođenja ekstrakcije podataka.

Nakon prepoznavanja uređaja od strane forenzičkog alata, otvara se novi prozor u kojem se korisnika obavještava da je uređaj uspješno identificiran, međutim za ovaj uređaj ne se pojavljuje više mogućih opcija kao u slučaju pametnog mobilnog terminalnog uređaja, već samo jedna opcija koju je moguće odabrati, što je prikazano na idućoj slici 7.



Slika 7. Sučelje forenzičkog alata *Oxygen Forensic Detective* nakon prepoznavanja nosivog terminalnog uređaja

Upravo kako je dostupna jedina moguća opcija za ekstrakciju podataka s nosivog terminalnog uređaja, ona se odabire te započinje proces ekstrakcije podataka, kako je prikazano slikom 8.



Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.

Slika 8. Postupak provođenja ekstrakcije podataka s nosivog terminalnog uređaja

Prilikom završetka procesa ekstrakcije podataka, otvara se obavijest unutar forenzičkog alata o ishodu procesa ekstrakcije podataka s identičnim opcijama kao što je navedeno u prethodnom primjeru kod pametnog mobilnog terminalnog uređaja, što je prikazano slikom 9.



Slika 9. Ishod procesa ekstrakcije podataka nosivog terminalnog uređaja

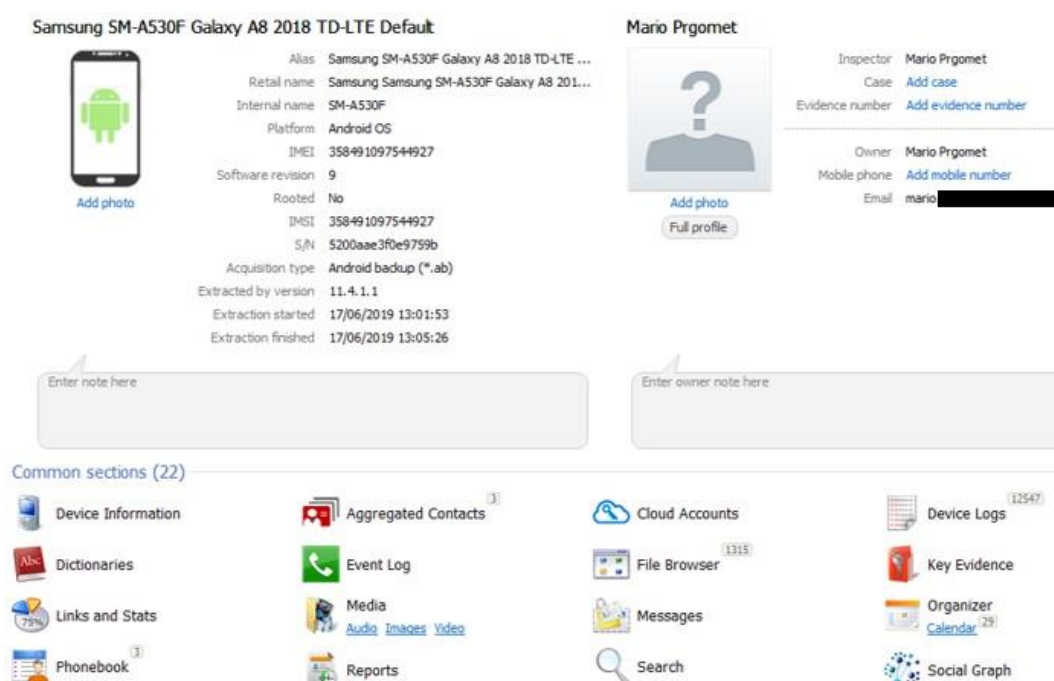
Povodom završetka procesa ekstrakcije podataka i generiranom obavijesti o njezinom ishodu, u idućem koraku forenzičke analize pristupa se analizi ekstrahiranih podataka.

6. Analiza ekstrahiranih podataka

Nakon prethodno odrađenog procesa forenzičke analize i ekstrakcije podataka s uređaja u prethodnom poglavlju, pristupa se detaljnoj analizi svih mogućih dobivenih ekstrahiranih podataka te se sagledavaju mogućnosti koje je moguće dobiti putem pojedine forenzičke metode.

6.1. Analiza ekstrahiranih podataka s pametnog mobilnog terminalnog uređaja

Prilikom započinjanja analize ekstrahiranih podataka, otvara se cjelokupan pregled prethodno obavljene ekstrakcije sa svim rezultatima i količinom podataka te osnovne informacije o uređaju koji je bio predmet ispitivanja, kako je prikazano na slici 5. Neovisno o odabranim i korištenim metodama u procesu ekstrakcije podataka, takav prozor će se uvijek pojaviti.



Slika 10. Rezultat ekstrakcije podataka pametnog mobilnog terminalnog uređaja

Kao najbolja opcija pokazala se metoda *Device acquisition*, koja nudi dvije varijante: zadani način rada te napredni način rada, kako je spomenuto u prethodnom poglavlju. Rezultati tih dviju varijanti su očekivano različiti. Međutim, ono što je neobično je to da je u zadanom načinu rada nasuprot naprednog, ekstrahirana nešto veća količina podataka u odjeljku *Device Logs*, što je prikazano na usporednoj slici 6. ovih dviju varijanti. Logika nalaže da bi u naprednom načinu rada ipak trebalo biti više ekstrahiranih podataka s uređaja, međutim u ovome slučaju to konkretno može ovisiti o trenutnom operacijskom sustavu na uređaju, verziji forenzičkog alata i njegovim

moogućnostima, ali i zbog ne korištenja nikakvih dodatnih opcija pristupa poput *root*¹⁵ pristupa i sličnih opcija. Upravo radi toga što je zadani način rada uspio rezultirati većom količinom ekstrahiranih podataka u daljnjem nastavku rada on će biti glavni predmet istraživanja i analize.



Slika 11. Usporedba metoda ekstrakcije podataka: zadani način rada (lijevo) i napredni način rada (desno)

U daljnjoj analizi ekstrahiranih podataka otkrilo se da je forenzički alat uspio izvući sljedeće podatke:

- e-mail adrese koje su se koristile na uređaju
- detalje i informacije o kontaktima na uređaju i povezanim korisničkim računima
- multimedijske datoteke (fotografije i audio datoteke)
- cjelokupan datotečni sustav uređaja s pripadajućim bazama podataka
- podatke s pojedinih aplikacija (zdravstvena fitness aplikacija *Runkeeper*).

Multimedijski podaci ekstrahirani u procesu ekstrakcije, prikazani slikom 12, predstavljeni su kroz fotografije i zvučne zapise. Ekstrahirani podaci tako su sadržani na pametnom mobilnom terminalnom uređaju i vidljivi su u slučaju provjere ili usporedbe podataka, dok se izbrisani podaci ovim tipom ekstrakcije nisu uspjeli pribaviti.

¹⁵ *Root* pristup - zadani administrativni korisnički račun koji omogućava pristup na uređaju kako bi se obavile radnje koje na uređaju obično nisu dopuštene

		Name ▲	Size	Extension	Modified (Device time) ▼	Type	Filter	Created (Device time) ▼
☒		MFSK_01.m4a	6.88 MB	.m4a	14/06/2019 09:29:25	MPEG-4 Audio	Audio	N/A
☒		MFSK_02.m4a	3.47 MB	.m4a	14/06/2019 09:29:25	MPEG-4 Audio	Audio	N/A
☒		Over_the_Horizon...	4.65 MB	.mp3	01/01/2017 20:42:49	MP3 Format Sound	Audio	N/A
		Name ▲	Size	E...	Modified (Device time) ▼	Type	Filter	Created (Device time) ▼
☒		20190413_175410...	632.27 KB	.jpg	13/04/2019 15:54:24	IrfanView JPG File	Images	N/A
☒		20190422_111206...	654.36 KB	.jpg	22/04/2019 18:29:54	IrfanView JPG File	Images	N/A
☒		20190422_111216...	733.75 KB	.jpg	22/04/2019 18:30:01	IrfanView JPG File	Images	N/A

Slika 12. Ekstrahirane multimedijske datoteke pametnog mobilnog terminalnog uređaja

Unutar forenzičkog alata moguće je prikazati cjelokupni datotečni sustav pametnog mobilnog terminalnog uređaja, koji je rezultat procesa ekstrakcije podataka s uređaja. Odabirom pojedinih stavki datotečnog sustava, otvara se mogućnost detaljnijeg pregleda sadržanih povezanih podataka i analize prisutnih baza podataka, što pokazuju slike 13 i 14.

☒		com.dsi.ant.sample.acquirechannels	N/A	Folder	N/A
☒		com.dsi.ant.service.socket	N/A	Folder	N/A
☒		com.fitnesskeeper.runkeeper.pro	N/A	Folder	N/A
☒		com.google.android.backuptransport	N/A	Folder	N/A
☒		com.google.android.ext.services	N/A	Folder	N/A
☒		com.google.android.feedback	N/A	Folder	N/A
☒		com.google.android.gms.policy_sidecar_aps	N/A	Folder	N/A
☒		com.google.android.onetimeinitializer	N/A	Folder	N/A
☒		com.mapmyrun.android2	N/A	Folder	N/A

Slika 13. Ekstrahirani datotečni sustav pametnog mobilnog terminalnog uređaja

Pristup proučavanju baza podataka omogućen je integriranom opcijom putem programa *SQLite Viewer*, koji je softverska podrška korištenog forenzičkog alata *Oxygen Forensic Detective*.

		Name ▲	Size	Extension	Modified (Device time) ▼	Type	Filter
☒		EventLog.sqlite	167.01 KB	.sqlite	17/06/2019 12:57:14	SQLITE File	Database files
☒		EventLog.sqlite-journal	166.79 KB	.sqlite-journal	17/06/2019 12:57:14	SQLITE-JOURNAL File	Other files
☒		RunKeeper.sqlite	2.14 MB	.sqlite	17/06/2019 12:18:29	SQLITE File	Database files
☒		RunKeeper.sqlite-journal	453.00 KB	.sqlite-journal	17/06/2019 12:18:29	SQLITE-JOURNAL File	Other files

Slika 14. Ekstrahirane baze podataka pametnog mobilnog terminalnog uređaja

U slučaju odabire jedne od ponuđenih ekstrahiranih baza podataka, kao što je vidljivo u okviru slike 14, otvara se odabrana baza podataka što predstavlja iduća

File Name	Offset	Hex	ASCII
android_metadata(1/0)	00026317-00027339	p , 0x00000000	p , 0x00000000
event(3/0)	00027349-00028371	\n 0x00000000	\n 0x00000000
prop(26/0)	00028381-00029403	Rn 0x00000000	Rn 0x00000000
sqlite_sequence(2/0)	00029413-00030435	dA 0x00000000	dA 0x00000000
All Deleted Data	00030445-00031467	^A 0x00000000	^A 0x00000000
	00031477-00032499	j 0x00000000	j 0x00000000
	00032509-00033531	QLite format 3	QLite format 3
	00033541-00034563	d j T e f	d j T e f
	00034573-00035595	^A 0x00000000	^A 0x00000000
	00035605-00036627	Y 0x00000000	Y 0x00000000
	00036637-00037659	Y8 0x00000000	Y8 0x00000000
	00037669-00038691	PA 0x00000000	PA 0x00000000
	00038701-00039723	K < + tY= 0x00000000	K < + tY= 0x00000000
	00039733-00040755	\n 0x00000000	\n 0x00000000
00000000:	00 00 00 1F 00 5E 00 03	E2 03 C4 03 A6 03 88 03	...^..A.A..^..
00000010:	7A 03 4C 02 3E 03 10 02	F2 04 D4 02 B6 02 98 02	j.L.....O.Q.?
00000020:	6A 02 5C 02 0E 02 20 02	02 01 E4 01 C6 01 A8 01	z.\>...&.E..
00000030:	8A 01 6C 01 4E 01 30 01	12 00 F4 00 D6 00 B8 00	\$.1.N.O...O.O..
00000040:	9A 00 7C 00 5E 00 00 00	00 00 00 00 00 00 00 00	\$. ^.....
00000050:	00 00 00 00 00 00 00 00	00 00 00 00 00 1B DE 1F	B
00000060:	05 00 02 33 0F 02 5A 4D	4D 42 49 4C 5F 52 45	...3..ZMOBILE_RE
00000070:	53 45 4E 54 5F 45 56 45	4E 54 31 1B DE 1E 05 00	SENT_EVENT1.B..
00000080:	02 33 0F 02 59 4D 4F 42	49 45 4C 5F 52 45 53 45	..3..ZMOBILE_RESE
00000090:	4E 54 5F 45 56 45 4E 54	31 1B DE 1D 05 00 02 33	NT_EVENT1.B...3..
000000A0:	0F 02 58 4D 4F 42 49 4C	45 5F 52 45 53 45 4E 54	..ZMOBILE_RESENT
000000B0:	5F 45 56 45 4E 54 31 1B	DE 1C 05 00 02 33 0F 02	_EVENT1.B...3..
000000C0:	57 4D 4F 42 49 4C 5F 52	52 45 53 45 4E 54 5F 45	ZMOBILE_RESENT E
000000D0:	56 45 4E 54 31 1B DE 1F	05 00 02 33 0F 02 56 4D	VENT1.B...3..YM

i dio forenzičke analize odnosi se na uspješno ekstrahirane podatke odjeljka *logs*. U sklopu tih podataka, koji su predstavljeni kao *log* zapisi tj. detaljni zapisi o događajima i aktivnostima na uređaju, mogu se pronaći važne informacije koje se mogu detaljnije. Primjerice, zapis sadrži podatke o tome koja se aktivnost u određenom trenutku odvijala (npr. trčanje), koje su aplikacije bile korištene, koji su uređaji u danom trenutku bili aktivni, je li se koristila Wi-Fi mreža (aktivan status ili ne), koji su korisnički računi (e-mail adrese) korišteni za prijave u pojedine aplikacije. Dio *log* zapisa prikazan je slikom 16.

```
+2h31m48s285ms (3) 097 040000a0 current=-14 ap_temp=23 pst_temp=27 bat_temp=26 chg_temp=27 pa_temp=-99 -running
+2h32m57s986ms (3) 097 800000a0 +running -wifi_radio wake_reason=0:"l56:s2mpu08-irq" stats=0:"wifi-data: inactive
+2h32m58s082ms (3) 097 c40000a0 +wake_lock=1001:"*telephony-radio*" +wifi_radio stats=0:"wifi-data: active
+2h32m58s542ms (2) 097 840000a0 -wake_lock stats=0:"get-stats
```

apisa uočen je redak o zapisu i informacijama *Bluetooth* u općem prikazu rezultata forenzičke analize ne navodi nikakve podatke o tome da postoji veza, iako su podaci povezani putem *Bluetooth* tehnologije. Međutim, u *log* zapisima vidljiva je jedna konekcija, što je prikazano slikom 17. Slika prikazuje povezivanje *Bluetooth* konekciji s pripadajućim podacima te je crvenom bojom istaknuta. U ovom slučaju se navodi povezani uređaj tj. pametni sat *Samsung SM-R200* čime se značajno pridonosi važnosti pregledavanja *log* datoteka.

```
04-11 21:51:17.486--BluetoothDataManager -- CONNECTION INFO : {"LO_MFN":"117","LO_LMP":
"9","LO_SUB":"0","LO_FWV":"f/w: 0|2925|2018-06-11 15:47:31 UTC|lassen_s612_lassen_a5_rev02_2017
07|R1-f23a-Jackpot","RE_OUI":"38:0B:40","RE_NAM":"Gear 2 (36F4)","RE_MFN":"15","RE_LMP":"6","RE_SUB":
"8707","RE_COD":"1796","RE_LTY":"1","RE_ROL":"1","RE_WEA":"1","CO_CFR":"","CO_ADR":"8","CO_HER":""}
```

Slika 17. Log zapis o *Bluetooth* konekciji s pametnim satom

Također, na slikama 18 te 19, prikazani su pojedini statistički podaci korištenih komunikacijskih tehnologija (*Bluetooth*, GPS te Wi-Fi) koji su pohranjeni u *log* zapisima datoteka.

GPS Statistics	
GPS signal quality (Top 4 Average CNO)	
poor (less than 20 dBHz):	13m 40s 472ms (0,1%)
good (greater than 20 dBHz):	8h 1m 7s 662ms (3,4%)
CONNECTIVITY POWER SUMMARY EN	
Bluetooth total received: 449,00KB, sent: 446,95K	
Bluetooth scan time: 9d 19h 7m 31s 575ms	
Bluetooth Idle time:	9d 11h 24m 42s 275ms (96,7%)
Bluetooth Rx time:	11h 49m 13s 810ms (5,0%)
Bluetooth Tx time:	3m 49s 602ms (0,0%)

Slika 18. Log zapisi statističkih podataka GPS i *Bluetooth* tehnologije

Primjerice, tako slika 18 prikazuje kvalitetu GPS signala te koliko se on vremenski koristio, dok za *Bluetooth* tehnologiju prikazuje količinu poslanih i primljenih podataka te ukupno vremensko korištenje, a na slici 19 je prikazana statistika korištenja Wi-Fi tehnologije uz zapise o aktivnosti, broju paketa, kvaliteti signala i ukupnom trajanju Wi-Fi konekcije.

Wifi Statistics	
Wifi kernel active time: 6h 30m 1s 186ms (2,8%)	
Wifi data received: 366,25M	
Wifi data sent: 56,84M	
Wifi packets received: 33719	
Wifi packets sent: 21961	
Wifi states	
scanning	4d 7h 33m 44s 966ms (44,0%)
disconn	12h 59m 59s 72ms (5,5%)
sta	4d 22h 33m 57s 911ms (50,4%)
Wifi Rx signal strength (RSSI)	
very poor (less than -88.75dBm):	4m 11s 580ms (0,0%)
poor (-88.75 to -77.5dBm):	2h 40m 38s 930ms (1,1%)
moderate (-77.5dBm to -66.25dBm):	3d 12h 16m 13s 179ms (35,8%)
good (-66.25dBm to -55dBm):	6d 2h 53m 13s 390ms (62,5%)
great (greater than -55dBm):	1h 13m 24s 870ms (0,5%)
WiFi Scan time:	36m 53s 569ms (0,3%)
WiFi Sleep time:	9d 10h 27m 37s 33ms (96,3%)
WiFi Idle time:	36m 59s 797ms (0,3%)

Slika 19. Log zapisi statističkih podataka o Wi-Fi tehnologiji

Važan rezultat u ekstrakciji podataka predstavlja i aplikacija *Runkeeper*. Upravo je *Runkeeper* zdravstvena fitness aplikacija bila povezana putem pametnog mobilnog terminalnog uređaja s pametnim satom i ovdje se otkrivaju prvi znakovi važnosti forenzičke analize koja je povezana s nosivim terminalnim uređajima. Na slici 20, prikazane su pojedine informacije o korištenju aplikacije *Runkeeper* koje zapravo otkrivaju veliku količinu podataka koji mogu biti interesantni forenzičkim istražiteljima. Osim što su iz aplikacije ekstrahirani podaci o korisniku aplikacije i njegovim osobnim podacima, vidljive su i rute njegova kretanja s podacima o prijeđenoj udaljenosti, vremenu početka aktivnosti, trajanju aktivnosti te tipu aktivnosti.

Account	Display name	Full name	Email	Birth date	Weight			
☒	Mario	Mario	pr-gi@net.hr	25/03/1996 ...	63.0 kg			
Activities	ID	Distance	Start time stamp (Device time)	Duration	Type	Calories	Notes	
☒	18	14185 m	17/06/2019 13:27:54	00:38:17	Cycling	410.95...	Hard	
☒	16	1593 m	14/06/2019 12:42:42	00:04:52	Cycling	35.0	N/A	
☒	15	1041 m	14/06/2019 12:38:45	00:02:48	Cycling	22.0	N/A	
☒	14	3024 m	14/06/2019 12:30:10	00:07:52	Cycling	64.0	Hot	
☒	10	10441 m	12/06/2019 12:54:38	00:58:46	Walking	445.0	Top	
☒	9	10374 m	12/06/2019 10:07:36	02:15:20	Walking	559.0	Good	
☒	8	10821 m	11/06/2019 13:15:14	01:26:21	Walking	504.0	Very well	
☒	7	10411 m	11/06/2019 10:07:59	01:16:09	Walking	474.0	Very well	
☒	4	19708 m	03/06/2019 12:17:43	11:50:51	Walking	1627.0	N/A	
☒	3	10547 m	03/06/2019 09:58:29	01:24:44	Walking	476.0	N/A	

Slika 20. Analiza ekstrahiranih podataka aplikacije *Runkeeper*

Tako postoje GPS podaci s geografskim koordinatama gdje se uređaj nalazio u određeno vrijeme. Kasnije prilikom odabira određene stavke unutar izbornika, u prozoru sa strane učitaju se detaljnije informacije o samome događaju koje uključuju brzinu kretanja, ali i zanimljivu opciju koja je omogućena forenzičkim alatom *Oxygen*, a to je da se lokacija povezuje s najbližim registriranim objektom (primjerice dućan, kafić ili tvrtka) kojeg je moguće pronaći na karti ili točno prezentiranom adresom, sve kako bi se omogućilo još preciznije lociranje gdje se korisnik nalazio, što je prikazano slikom 21.

☒	45.7813952956349;15.9327994845808	Jarun, Trešnjevka - jug, Zagreb, Grad Zagreb, 10000, Hrvatska
☒	45.7819141773507;15.9342187922448	Jarunska obala, Jarun, Trešnjevka - jug, Zagreb, Grad Zagreb, 10.000, Hrvatska
☒	45.8039711974561;16.0206204559654	Ivanićgradska, Ulica grada Vukovara, Volovčica, Peščenica - Žitnjak, Zagreb, Grad Zagreb, 10000 ZAGREB, Hrvatska
☒	45.7866181014106;15.9519117325544	Jadranski most, Knežija, Trešnjevka - jug, Zagreb, Grad Zagreb, 10000, Hrvatska
☒	45.8046970702708;16.035657087341	INA Zagreb-Žitnjak-Badel, 2, Ulica Marijana Čavića, Borongaj, Peščenica - Žitnjak, Zagreb, Grad Zagreb, 10000, Hrvatska
☒	45.8039135299623;16.0202549211681	iNovine, Ivanićgradska ulica, Ferenšćica, Peščenica - Žitnjak, Zagreb, Grad Zagreb, 10000 ZAGREB, Hrvatska

Slika 21. Korelacija geografske lokacije s registriranim objektom u blizini

Važnu stavke koje su pronađene unutar *Runkeeper* aplikacije predstavljaju određeni izbrisani podaci tj. GPS lokacije prikazane na slici 22.

☒			RunKeeper route	12/06/2019 13:48:56		45.7880084076896;15.9374261274934
☒			RunKeeper route	12/06/2019 13:49:03		45.7879283186048;15.937491171062
☒			RunKeeper route	12/06/2019 13:49:10		45.7878510374576;15.9375593997538
☒			RunKeeper route	12/06/2019 13:49:15		45.7877866644412;15.9376305621117
☒			RunKeeper route	12/06/2019 13:49:21		45.7877566153184;15.9377434663475
☒			RunKeeper route	12/06/2019 13:49:27		45.7877381332219;15.9378572087735
☒			RunKeeper route	12/06/2019 13:49:33		45.7877042284235;15.9379746392369

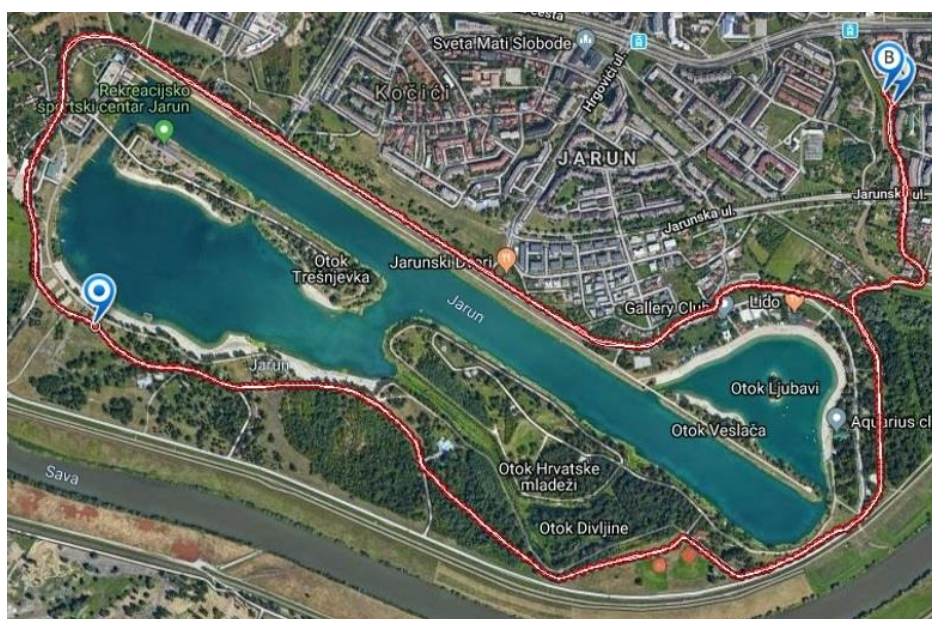
Slika 22. Izbrisani podaci otkriveni forenzičkim alatom *Oxygen Forensic Detective*

Osim što postoje izbrisane lokacije koje su s punim i točnim prikazom datuma i vremena kada se korisnik nalazio na toj lokaciji, postoje i pojedine lokacije kojima su postavke datuma i vremena predefinirani u 01. siječnja.1970. i 02:00:00, što je također vidljivo na slici 23. Takve postavke predstavljaju problem točnog vremenskog utvrđivanja kada se korisnik nalazio na toj lokaciji i izazov za forenzičke istražitelje.

☒		RunKeeper route	01/01/1970 02:00:00		45.8282874757424;16.0089653357863
☒		RunKeeper route	01/01/1970 02:00:00		45.8282829076052;16.0090646613389
☒		RunKeeper route	01/01/1970 02:00:00		45.8282249886543;16.0089228395373
☒		RunKeeper route	01/01/1970 02:00:00		45.8282003877685;16.0090112686157
☒		RunKeeper route	01/01/1970 02:00:00		45.828188569285;16.009048903361

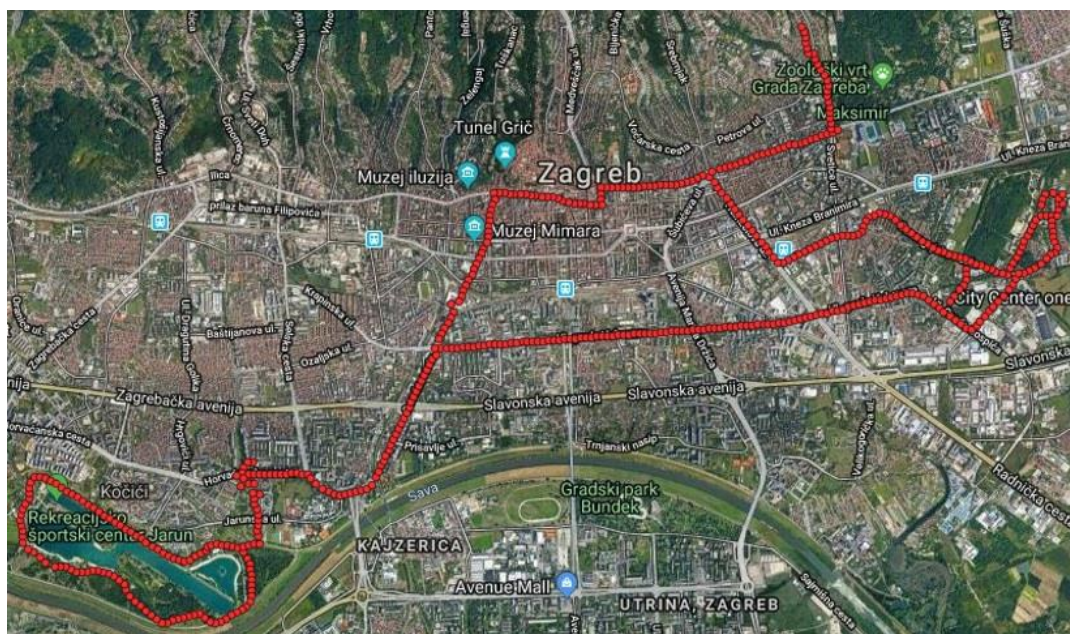
Slika 23. Resetiranje postavki vremenskih oznaka

Iduća izvrsna mogućnost pružena forenzičkim alatom *Oxygen Forensic Detective* je otvaranje GPS lokacija uređaja unutar geografske karte, što je prikazano na slici 24. Kako postoji mogućnost pregledavanja ruta korisnika, tako se one i ocrtavaju na mapi. Postoje točke A i B, koje predstavljaju početak i kraj rute, dok se odabirom određene točke na liniji rute otvaraju dodatne informacije koliko se korisnik puta nalazio na toj lokaciji i u kojem vremenu, drugim riječima zabilježen je svaki podatak za određenu GPS koordinatu.



Slika 24. Linijska ruta kretanja korisnika

Kvalitetna značajka forenzičkog alata je i ta da je moguće ekstrahirati apsolutno sve lokacije na kojima se korisnik nalazio prilikom korištenja uređaja i to predložiti na karti pomoću forenzičkog alata, kako je prikazano na sljedećoj slici 25.

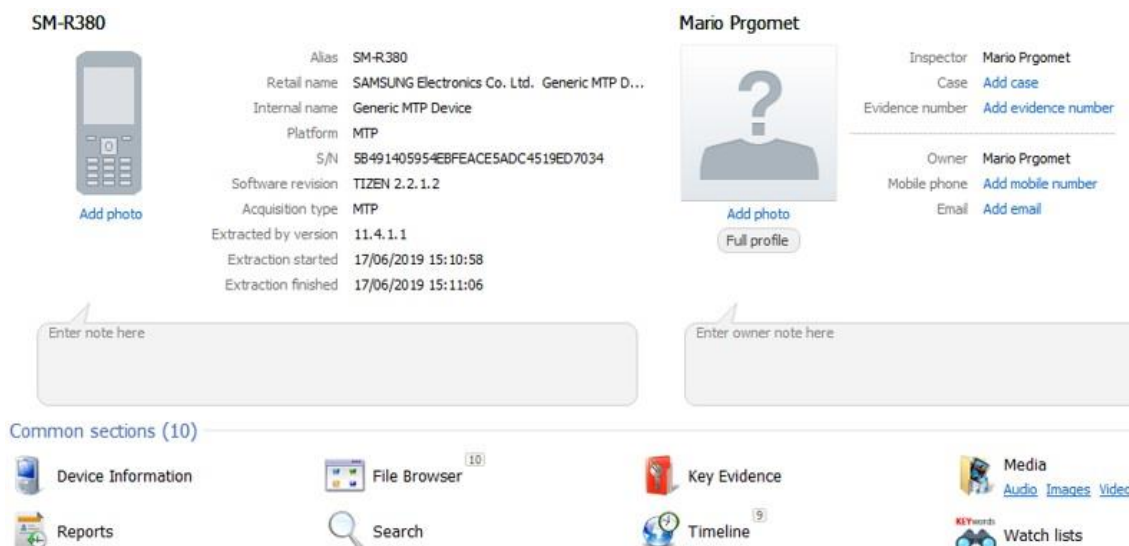


Slika 25. Točkasti prikaz svih dostupnih lokacija korisnika

Ovim poglavljem prikazani su rezultati procesa forenzičke analize i ekstrakcije podataka pametnog mobilnog terminalnog uređaja *Samsung Galaxy A8*. Važno je istaknuti da su se uspjeli ekstrahirati pojedini izbrisani podaci, ali i ostali koji mogu postati potencijalni predmet proučavanja.

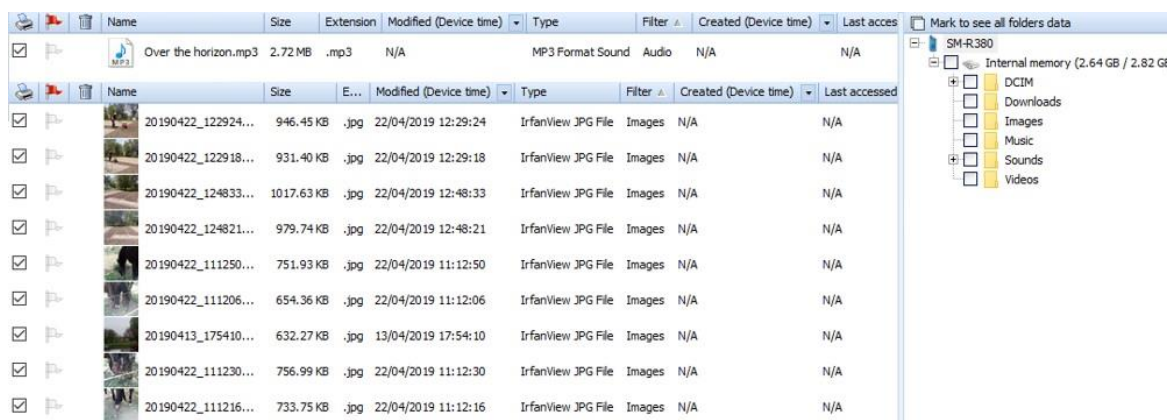
6.2. Analiza ekstrahiranih podataka s nosivog terminalnog uređaja

Ekstrahirani podaci s nosivog terminalnog uređaja dostupni su u značajnije manjoj količini nego što je to slučaj s pametnim mobilnim terminalnim uređajem, što je vidljivo na slici 26, prilikom otvaranja cjelokupnog pregleda rezultata napravljene ekstrakcije.



Slika 26. Rezultat ekstrakcije podataka nosivog terminalnog uređaja

Analizom ekstrahiranih podataka utvrđeno je da je napravljena jedina moguća forenzička metoda za ekstrakciju podataka s ovoga uređaja, a to je logička ekstrakcija. Tim putem dobio se uvid u osnovne informacije o uređaju, multimedijske datoteke (fotografije snimljene putem pametnog sata te audio datoteke) te datotečni sustav uređaja, što je prikazano slikom 27.



Slika 27. Ekstrahirani datotečni sustav i multimedijske datoteke nosivog terminalnog uređaja

U ovome poglavlju prikazani su rezultati procesa forenzičke analize i ekstrakcije podataka nosivog terminalnog uređaja odnosno pametnog sata *Samsung SM-R380 Gear 2*. Vidljiva je značajna razlika u rezultatima ekstrakcije podataka nosivog terminalnog uređaja i prethodnog poglavlja u kojem je obrađena forenzička analiza i

ekstrakcija podataka pametnog mobilnog terminalnog uređaja. Osim što se ostvario pristup multimedijским datotekama i datotečnom sustavu pametnog sata, ostali podaci nisu se pokazali dostupnima prilikom korištenja forenzičkog alata *Oxygen Forensic Detective* i njegovih mogućnosti.

6.3. Diskusija o dobivenim rezultatima

Analizom ekstrahiranih podataka i prezentiranim rezultatima dobiva se uvid i dojam u kompleksnost cjelokupne aktivnosti povezane s procesom forenzičke analize. Tako za određene dobivene i predložene podatke možemo tvrditi kako su i zbog čega nastali te objasniti njihov zapis, dok za neke od njih postoje samo pretpostavke i nagađanja. Upravo kroz prethodne odlomke spomenuti su neki od njih te su pojedine stavke postale vidljive tek nakon detaljnijeg pregleda ekstrahiranih podataka, što potvrđuje da je forenzička analiza iznimno kompleksan posao i potrebno ga je detaljno odraditi.

Uz mnoštvo ekstrahiranih podataka, uspjelo se doći i do određenih izbrisanih stavki. Količina ekstrahiranih podataka, ali i mogućnost pristupa izbrisanim podacima može ovisi o raznim utjecajima. U tom pogledu konkretno se govori o novim verzijama uređaja s novim razvijenim inačicama operativnih sustava. Određeni novi operativni sustavi koriste naprednije sigurnosne značajke kako bi se očuvali korisnički podaci te kako bi se općenito onemogućio pristup podacima nekim drugim osobama, podrazumijevajući i forenzičke istražitelje. Naprednije sigurnosne značajke uglavnom se baziraju na jačoj enkripciji podataka i aplikacija sustava.

Isto tako, važnu ulogu u procesu ekstrakcije podataka imaju i forenzički alati. Određene mogućnosti forenzičkih alata nisu u potpunosti razvijene kako bi pratile razvoj uređaja nad kojima je potrebno izvršiti ekstrakciju podataka i tako se ne može dobiti cjelokupna slika forenzičke analize. U određenim procesima forenzičke analize, iznimno je teško ostvariti pristup uređaju koji je potreban za izvršavanje ekstrakcije podataka. Težak pristup govori o potrebi za upotrebom i omogućavanjem dodatnih opcija za pristup uređaju, koje za mnoge uređaje nisu dostupne ili ih je nemoguće provesti.

Nadalje, u generalnim rezultatima forenzičke analize ne navodi se konekcija Bluetooth tehnologije, dok je detaljnijim pregledom *log* zapisa utvrđena njezina postojanost. Ovim putem je prezentirana važnost detaljnog proučavanja i analiziranja ekstrahiranih podataka, ali i pojedine mane unutar forenzičkog alata. U procesu forenzičke analize svi podaci bi se trebali detaljno pregledati, jer se u suprotnom mogu preskočiti određene stavke i podaci od interesa, dok je unutar forenzičkog alata potrebno povezati pojedine podatke u određenim odjeljcima kako bi se precizno sumirali cjelokupni podaci. Zanimljiva je činjenica što je putem tih zapisima također moguće otkriti da stvarna lokacija ne bazira samo na temelju GPS lokacije već i na temelju korištenja Wi-Fi mreža, bez obzira je li uređaj povezan na koju od njih ili nije, jer se u pozadini tokom aktivnosti cijelo vrijeme pokreće skeniranje okoline radi pružanja preciznije usluge lociranja.

Iduća stavka govori o mogućnosti kreiranja profila korisnika. U takvim situacijama i detaljnom analizom korisničkih podataka, poput GPS lokacija ili zapisa aktivnosti, moguće je stvoriti detaljan profil korisnika. Unutar profila korisnika tako se mogu otkriti specifične pojave njegova kretanja poput vremena dolaska ili odlaska s radnog mjesta, vremena određenih aktivnosti, vremena mirovanja čime se može utvrditi čak i mjesto

stanovanja. Kreiranjem detaljnog profila mogu se utvrditi rutine ili svakodnevnica korisnika pa tako profil može biti od izrazite pomoći tijekom određenih kriminalističkih istraga.

Također, prilikom pregleda ekstrahiranih podataka uočene su pojedine promjene u određenim podacima. Takav slučaj zabilježen je kod promjene datuma određenih GPS lokacija unutar aplikacije *Runkeeper*. Naime, aplikacija nije izbrisala te lokacije već je njihov datum resetiran prema postavkama aplikacije. Razlog promjeni datuma nije utvrđen i ne postoji objašnjenje za koje je lokacije to napravljeno i zašto. Međutim, moguće je da to ovisi o korištenoj aplikaciji i razvojnim programerima koji su odgovorni za pisanje koda aplikacije.

Kao što je ranije spomenuto, rezultat ekstrakcije nosivog terminalnog uređaja iznimno je ograničavajući. Jedina pretpostavka je ta da korišteni model pametnog sata nije u potpunosti podržan unutar dostupne verzije forenzičkog alata kako bi se izvršio cjelokupni pregled uređaja. Razlog tomu može biti korištenje drugačijeg operativnog sustava uređaja koji je posebno namijenjen za nosive terminalne uređaje ili zbog drugačijeg koncepta uređaja nego što su to pametni mobilni terminalni uređaji radi kojeg su oni temeljitije obrađeni u procesu forenzičke analize. Iako nosivi terminalni uređaji postaju najkorišteniji uređaji, u forenzičkoj analizi nisu toliko popularni, a trebali bi to postati zbog potencijala koji mogu predstaviti kroz podatke koji se na njima nalaze.

7. Zaključak

Vrlo ubrzan napredak tehnologije i raznolikost novih proizvoda predstavljaju izazov za forenzičku analizu koja mora pratiti razvoj softvera i hardvera, to jest novih vrsta uređaja, tržišnih proizvoda. Zato je forenzička analiza vrlo dinamično područje koje stalno analizira proizvode i traži alate za analizu podataka koje generiraju. Razumljivo, za to potrebno vrijeme, pa je forenzika, primjerice, na području nosivih terminalnih uređaja još u razvoju. Vjerojatno u vječnom razvoju, jer na tržište će se plasirati novi i novi proizvodi.

Raznovrsnost uređaja, kapacitet pohrane podataka i multifunkcionalnost uređaja čine nosive terminalne uređaje potencijalno korisnima za forenzičke analize u sklopu eventualnih kriminalističkih istraga. Odnosi se to na sve uređaje pa tako i na nosive terminalne uređaje kao što su pametni satovi, narukvice te uređaji koji se ugrađuju u obuću i odjeću. Mnogi od nosivih uređaja imaju ograničen kapacitet pohrane, njihovo je korištenje povezano s drugim uređajima, npr. pametnim mobilnim terminalnim uređajima, ali i sami mogu pohraniti relevantne podatke korisne za eventualne istrage.

U ovome je radu prikazan postupak forenzičke analize s ciljem ekstrakcije i prikupljanja podataka iz nosivog terminalnog uređaja odnosno pametnog sata te pripadajućeg povezanog pametnog mobilnog terminalnog uređaja, kako bi se mogla izvršiti potrebna forenzička analiza dostupnih podataka. Razni faktori mogu utjecati na moguću količinu ekstrahiranih podataka. Primjerice, koliko će se korisnim pokazati antiforenzičke metode kako bi se utjecalo na onemogućavanje pronalaska podataka, koje dodatne opcije treba omogućiti na uređajima kako bi se dobio potpuniji uvid u pohranjene podatke ili koliko su snažni operativni sustavi u zaštiti korisničkih podataka putem enkripcijskih metoda. Forenzička akvizicija nosivih te mobilnih terminalnih uređaja može predstavljati kritičnu točku u cjelokupnoj istrazi, dok će forenzička analiza ovih vrsta uređaja u nekim slučajevima bit će od iznimne važnosti.

U provedenom istraživanju i forenzičkoj analizi pametnog mobilnog terminalnog uređaja - *Samsung Galaxy A8* i nosivog terminalnog uređaja, pametnog sata - *Samsung SM-R380 Gear 2*, za ekstrakciju podataka i njihovu analizu korišten je forenzički alat *Oxygen Forensic Detective*. Utvrđeno je da trenutno dostupni forenzički alati daju tek ograničenu podršku prilikom forenzičke analize nosivih terminalnih uređaja. Iako zbog toga u praksi ovi uređaji nisu u prvome planu, istraživanje je pokazalo kako je analizom moguće prikupiti relevantne informacije. Primjerice, mjesto, položaj korisnika uređaja u prostoru u određenom vremenu, smjer njegova kretanja, podaci povezani s aplikacijama, kontakti, multimedijски sadržaji itd., a svi ti podaci mogu biti vrlo važni digitalni dokazi u eventualnim kriminalističkim istragama.

Prezentiranim potencijalom pretpostavka je da će navedeni uređaji odigrati značajnu ulogu u budućnosti te svojim postojanjem pridonijeti cjelokupnom procesu forenzičke analize.

Popis literature

[1] Reiber, L.: *Mobile Forensic Investigation: A Guide to Evidence Collection, Analysis, and Presentation, Second Edition*, McGraw-Hill Education, SAD, 2018.

[2] URL: <https://www.statista.com/topics/1556/wearable-technology/> (pristupljeno: lipanj 2019.)

[3] URL: <https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/> (pristupljeno: lipanj 2019.)

[4] URL: <https://www.gartner.com/en/documents/3891988/forecast-wearable-electronic-devices-worldwide> (pristupljeno: lipanj 2019.)

[5] URL: <https://www.statista.com/statistics/610447/wearable-device-revenue-worldwide/> (pristupljeno: lipanj 2019.)

[6] URL: <https://www.gartner.com/en/newsroom/press-releases/2018-11-29-gartner-says-worldwide-wearable-device-sales-to-grow-> (pristupljeno: srpanj 2019.)

[7] URL: <https://www.globalsources.com/gsol//Activity-tracking/a/9000000132594.html> (pristupljeno: srpanj 2019.)

[8] Yang, B.: *Bluetooth: Technology and Applications*, CTTL-System Laboratory, China Academy of Information and Communication Technology, Kina, 2017.

[9] Stirparo, P., Loeschner, J., Cattani, M.: *Bluetooth technology: security features, vulnerabilities and attacks*, 2012.

[10] URL: <https://www.tomshardware.co.uk/bluetooth-technology-101,review-33507.html#p1> (pristupljeno: srpanj 2019.)

[11] URL: <https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html> (pristupljeno: srpanj 2019.)

[12] URL: <https://www.wi-fi.org/discover-wi-fi> (pristupljeno: srpanj 2019.)

[13] URL: <https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html> (pristupljeno: srpanj 2019.)

[14] Dordal, P. L.: *An Introduction to Computer Networks, Release 1.9.19*, Department of Computer Science, Loyola University, Chicago, SAD, 2019.

[15] URL: <https://www.intel.com/content/www/us/en/support/articles/000005725/network-and-io/wireless-networking.html> (pristupljeno: srpanj 2019.)

[16] URL: <http://nearfieldcommunication.org/about-nfc.html> (pristupljeno: srpanj 2019.)

- [17] URL: <http://nearfieldcommunication.org/how-it-works.html> (pristupljeno: srpanj 2019.)
- [18] URL: <http://nearfieldcommunication.org/using-nfc.html> (pristupljeno: srpanj 2019.)
- [19] URL: <http://nearfieldcommunication.org/technology.html> (pristupljeno: srpanj 2019.)
- [20] Hoque, Z.: *Basic Concept of GPS and Its Applications*, IOSR Journal Of Humanities And Social Science (IOSR-JHSS), Volume 21, Issue 3, Ver. II, 2016.
- [21] Vail, J., Parsons, M., Striggow, B.: *Global Positioning System*, U.S. Environmental Protection Agency, Science and Ecosystem Support Division, SAD, 2015.
- [22] URL: <https://galileognss.eu/how-many-galileo-satellites-are-now-in-orbit/> (pristupljeno: srpanj 2019.)
- [23] Muštra, M.: *Autorizirana predavanja iz kolegija Lokacijski i navigacijski sustavi*, Fakultet prometnih znanosti, Hrvatska, 2018.
- [24] Doherty, E. P.: *Digital Forensics for Handheld Devices*, CRC Press, Taylor & Francis Group, SAD, 2013.
- [25] URL: <http://web.studenti.math.pmf.unizg.hr/~marrast/Senzori> (pristupljeno: srpanj 2019.)
- [26] URL: <https://www.globalsources.com/gsol//Activity-tracking/a/9000000132594.html> (pristupljeno: srpanj 2019.)
- [27] Hayward, J.: *Wearable Sensors 2018-2028: Technologies, Markets & Players*, IDTechEx, Ujedinjeno Kraljevstvo, 2017.
- [28] Malmivaara, M.: *The Emergence of Wearable Computing*, Tampere University of Technology, Finska, 2009.
- [29] Hurford, R. D.: *Types of Smart Clothes and Wearable Technology*, University of Wales Newport, Ujedinjeno Kraljevstvo, 2009.
- [30] ENISA: *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, 2017.
- [31] Parikh, S., Chavda, D., Chakraborty, S., Rughani, P. H., Dahiya, M. S.: *Analysis of Android Smart Watch Artifacts*, International Journal of Scientific & Engineering Research, Volume 6, Issue 8, 2015.
- [32] Alabdulsalam, S., Schaefer, K., Kechadi, T., Le-Khac, N. A.: *Internet of Things Forensics: Challenges and Case Study*, 2018.
- [33] Chernyshev, M., Zeadally, S., Baig, Z., Woodward, A.: *Internet of Things Forensics: The Need, Process Models, and Open Issues*, IEEE, IT Professional, Volume 20, Issue 3, 2018.

- [34] Casey, E.: *Handbook of Digital Forensics and Investigation*, Academic Press, 2010.
- [35] Bommisetty, S., Tamma, R., Mahalik, H.: *Practical Mobile Forensics*, Packt Publishing, Birmingham, Ujedinjeno Kraljevstvo, 2014.
- [36] Murphy, C. A.: *Developing Process for Mobile Device Forensics*, 2015.
- [37] U.S. Department of Homeland Security: *NIST Mobile Forensics Workshop and Webcast: Mobile Device Forensics: A - Z*, SAD, 2014.
- [38] Hoog, A.: *Android Forensics: Investigation, Analysis, and Mobile Security for Google Android*, Elsevier, SAD, 2011.
- [39] Tamma, R., Tindall, D.: *Learning Android Forensics*, Packt Publishing, Birmingham, Ujedinjeno Kraljevstvo, 2015.
- [40] URL: <https://blog.specialcounsel.com/ediscovery/three-types-of-mobile-device-extractions-and-what-each-contains/> (pristupljeno: kolovoz 2019.)
- [41] Cellebrite: *What Happens When You Press that Button? Explaining Cellebrite UFED Data Extraction Processes*, 2014.
- [42] Tahiri, S.: *Mastering Mobile Forensics*, Packt Publishing, Birmingham, Ujedinjeno Kraljevstvo, 2016.
- [43] Mikhaylov, I.: *Mobile Forensics Cookbook*, Packt Publishing, Birmingham, Ujedinjeno Kraljevstvo, 2017.
- [44] Ćosić, J., Ćosić, Z., Bača, M.: *Digitalna antiforenzika - manipulacija procesom digitalne istrage*, 18. Telekomunikacioni forum TELFOR 2010., Beograd, Srbija, 2010.
- [45] Gogolin, G.: *Digital Forensics Explained*, CRC Press, Taylor & Francis Group, SAD, 2013.
- [46] Graves, M. W.: *Digital Archaeology: The Art and Science of Digital Forensics, First Edition*, Pearson Education, SAD, 2014.
- [47] Casey, E., Turnbull, B.: *Digital Evidence on Mobile Devices*, 2011.
- [48] URL: <https://www.csoononline.com/article/2117658/rules-of-evidence---digital-forensics-tools.html> (pristupljeno: kolovoz 2019.)
- [49] U.S. Department of Homeland Security: *Digital Forensics Tools*, SAD, 2016.
- [50] URL: <https://www.oxygen-forensic.com/en/company> (pristupljeno: kolovoz 2019.)
- [51] Oxygen Forensics: *Oxygen Forensic Detective: Getting Started Guide*, 2019.
- [52] Oxygen Forensics: *Oxygen Forensic Detective 11.1*, 2018.
- [53] Oxygen Forensics: *Oxygen Forensic Detective 11.0*, 2018.

[54] URL: https://www.oxygen-forensic.com/uploads/doc_guide/Oxygen_Forensic®_Detective_-_Device_Data_Analysis1.pdf (pristupljeno: kolovoz 2019.)

[55] Baggili, I., Oduru, J., Anthony, K., Breiting, F., McGee, G.: *Watch What You Wear: Preliminary Forensic Analysis of Smart Watches*, 10th International Conference on Availability, Reliability and Security, SAD, 2015.

[56] Rongen, J., Geradts, Z.: *Extraction and Forensic Analysis of Artifacts on Wearables*, International Journal of Forensic Science & Pathology, 2017., 312-318.

[57] URL: <https://abrignoni.blogspot.com/2018/08/android-nike-run-app-geolocation-sqlite.html> (pristupljeno: kolovoz 2019.)

Popis kratica

API	(<i>Application Programming Interface</i>) aplikacijsko programsko sučelje
AR	(<i>Augmented Reality</i>) proširena stvarnost
ASCII	(<i>American Standard Code for Information Interchange</i>) znakovni kod
BR/EDR	(<i>Basic Rate/Enhanced Data Rate</i>) osnovna/poboljšana brzina prijenosa podataka
CPEEP	(<i>Cellular Phone Evidence Extraction Process</i>) proces ekstrakcije dokaza s mobilnih terminalnih uređaja
CPU	(<i>Control Processing Unit</i>) procesorska jedinica
EEG	(<i>Electroencephalography</i>) elektroencefalogram
EKG	(<i>Electrocardiography</i>) elektrokardiogram
EMG	(<i>Electromyography</i>) elektromiografija
eMMC	(<i>Embedded Multi Media Controller</i>) memorijski čip koji integrira <i>flash</i> memoriju i kontroler u jedan modul
ESN	(<i>Electronic Serial Number</i>) elektronički serijski broj
GLONASS	(<i>Globalnaja Navigacionaja Sputnjikova Sistema</i> ili <i>Global Navigation Satellite System</i>) globalni navigacijski satelitski sustav
GPS	(<i>Global Positioning System</i>) globalni položajni sustav
GSM	(<i>Global System for Mobile Communications</i>) druga generacija digitalnog globalnog sustava mobilne mreže
IBM	(<i>International Business Machines</i>) Američka multinacionalna tvrtka za informacijsku tehnologiju
IEEE	(<i>Institute of Electrical and Electronics Engineers</i>) Institut inženjera elektrotehnike i elektronike
IM	(<i>Instant Messaging</i>) platforma za slanje poruka
IMEI	(<i>International Mobile Equipment Identity</i>) međunarodni identifikator mobilnog uređaja
IMSI	(<i>International Mobile Subscriber Identity</i>) međunarodni identifikator mobilnog pretplatnika
IoT	(<i>Internet of Things</i>) Internet stvari
IRNSS	(<i>Indian Regional Navigation Satellite System</i>) Indijski regionalni navigacijski satelitski sustav
ISP	(<i>In-System Programming</i>) programiranje unutar sustava
JTAG	(<i>Joint Test Action Group</i>) zajednička akcijska grupa za testiranje, metoda forenzičke ekstrakcije
LE	(<i>Low Energy</i>) niska potrošnja energije
LTE	(<i>Long-Term Evolution</i>) četvrta generacija digitalnog globalnog sustava mobilne mreže
MEID	(<i>Mobile Equipment Identifier</i>) identifikator mobilne opreme
MMS	(<i>Multimedia Messaging Service</i>) multimedijske poruke
MSISDN	(<i>Mobile Station International Subscriber Directory Number</i>) međunarodni telefonski broj pretplatnika mobilne stanice

NAVSTAR	<i>(Navigation System with Time And Ranging Global Positioning System)</i> navigacijski sustav s vremenskim i rasponskim globalnim položajnim sustavom
NFC	<i>(Near Field Communication)</i> komunikacija bliskog polja
PIN	<i>(Personal Identification Number)</i> osobni broj korisnika
QZSS	<i>(Quasi-Zenith Satellite System)</i> satelitski sustav Quasi-Zenith
RFID	<i>(Radio Frequency Identification)</i> radio frekvencijska identifikacija
RJ-45	<i>(Registered Jack 45)</i> standardni priključak za prijenos podataka
RS-232	<i>(Recommended Standard 232)</i> standard podatkovnih kablova
SIG	<i>(Special Interest Group)</i> trgovinsko udruženje koje se bavi Bluetooth standardima
SIM	<i>(Subscriber Identity Module)</i> modul identiteta pretplatnika, SIM kartica
SMS	<i>(Short Message Service)</i> tekstualne poruke
TAP	<i>(Test Access Port)</i> standardni testni pristupni priključak
UICC	<i>(Universal Integrated Circuit Card)</i> vrsta SIM kartice koja se koristi za drugu (GSM) ili treću (UMTS) generaciju mobilne mreže
USB	<i>(Universal Serial Bus)</i> univerzalna serijska sabirnica
VR	<i>(Virtual Reality)</i> virtualna stvarnost

Popis slika

Slika 1. Senzori nosivih terminalnih uređaja

Slika 2. Faze procedure postupka ekstrakcije dokaza

Slika 3. Piramidalna struktura klasifikacije metoda ekstrakcije podataka

Slika 4. Sučelje forenzičkog alata *Oxygen Forensic Detective* nakon prepoznavanja pametnog mobilnog terminalnog uređaja

Slika 5. Postupak provođenja ekstrakcije podataka s pametnog mobilnog terminalnog uređaja

Slika 6. Ishod procesa ekstrakcije podataka pametnog mobilnog terminalnog uređaja

Slika 7. Sučelje forenzičkog alata *Oxygen Forensic Detective* nakon prepoznavanja nosivog terminalnog uređaja

Slika 8. Postupak provođenja ekstrakcije podataka s nosivog terminalnog uređaja

Slika 9. Ishod procesa ekstrakcije podataka nosivog terminalnog uređaja

Slika 10. Rezultat ekstrakcije podataka pametnog mobilnog terminalnog uređaja

Slika 11. Usporedba metoda ekstrakcije podataka: zadani način rada (lijevo) i napredni način rada (desno)

Slika 12. Ekstrahirane multimedijske datoteke pametnog mobilnog terminalnog uređaja

Slika 13. Ekstrahirani datotečni sustav pametnog mobilnog terminalnog uređaja

Slika 14. Ekstrahirane baze podataka pametnog mobilnog terminalnog uređaja

Slika 15. Pregled baze podatak putem programa *SQLite Viewer*

Slika 16. Parcijalni *log* zapis

Slika 17. *Log* zapis o *Bluetooth* konekciji s pametnim satom

Slika 18. *Log* zapisi statističkih podataka GPS i *Bluetooth* tehnologije

Slika 19. *Log* zapisi statističkih podataka o Wi-Fi tehnologiji

Slika 20. Analiza ekstrahiranih podataka aplikacije *Runkeeper*

Slika 21. Korelacija geografske lokacije s registriranim objektom u blizini

Slika 22. Izbrisani podaci otkriveni forenzičkim alatom *Oxygen Forensic Detective*

Slika 23. Resetiranje postavki vremenskih oznaka

Slika 24. Linijska ruta kretanja korisnika

Slika 25. Točkasti prikaz svih dostupnih lokacija korisnika

Slika 26. Rezultat ekstrakcije podataka nosivog terminalnog uređaja

Slika 27. Ekstrahirani datotečni sustav i multimedijske datoteke nosivog terminalnog uređaja

Popis grafikona

Grafikon 1. Statistička analiza broja prodanih nosivih terminalnih uređaja u svijetu

Grafikon 2. Prihod od prodaje nosivih terminalnih uređaja u svijetu od 2012. do 2022. godine

Popis tablica

Tablica 1. Osnovne karakteristike verzija Wi-Fi tehnologije

Tablica 2. Kategorička podjela nosivih terminalnih uređaja