Forenzika pametnog telefona temeljena na podacima Google usluga

Grgić, Ivan

Master's thesis / Diplomski rad

2022

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:119:788545

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-29**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

Sveučilište u Zagrebu

Fakultet prometnih znanosti

Ivan Grgić

FORENZIKA PAMETNOG TELEFONA TEMELJENA NA PODACIMA GOOGLE USLUGA

DIPLOMSKI RAD

Zagreb, rujan 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 16. ožujka 2022.

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

DIPLOMSKI ZADATAK br. 6648

Pristupnik: **Ivan Grgić (0135241780)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Forenzika pametnog telefona temeljena na podacima Google usluga**

Opis zadatka:

Analizirati primjenu pametnih telefona i povezanih digitalnih dokaza. Diferencirati značajke alata za forenzičku analizu uređaja i aplikacija. Preispitati Google usluge primijenjene na pametnim telefonima. Prikazati ekstrakciju podataka Google usluga. Analizirati prikupljene podatke Google usluga pametnog telefona.

Mentor:

doc. dr. sc. Siniša Husnjak

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

FORENZIKA PAMETNOG TELEFONA TEMELJENA NA PODACIMA GOOGLE USLUGA

SMARTPHONE FORENSIC BASED ON DATA FROM GOOGLE SERVICES

Mentor: doc.dr.sc. Siniša Husnjak

Student: Ivan Grgić

JMBAG: 0135241780

Zagreb, rujan 2022.

SAŽETAK:

Pametni telefoni danas su dio svakodnevice i koriste se u različite svrhe, a ne samo za pozive ili poruke, kako je to bilo prvobitno namijenjeno korištenjem telefona. Različite aktivnosti i djelatnosti iziskuju korištenje pametnih telefona, a kao posljedica široke primjene i korištenja je kreiranje velike količine podataka. Razvojem forenzičkih alata, omogućena je ekstrakcija podataka koje prikupljaju pojedine aplikacije i Google usluge na pametnim telefonima. To su primjerice korisnički podaci, privatne poruke, trenutna lokacija uređaja i posjećene lokacije tog istog uređaja. U diplomskom radu obavljen je postupak ekstrakcije podataka temeljenim na Google uslugama korištenjem UFED Touch 2 forenzičkog alata. Analiza podataka dobivenih ekstrakcijom obavit će se korištenjem Cellebrite Reader alata. Koristi se referentna metodologija forenzičke analize mobilnih uređaja.

KLJUČNE RIJEČI: pametni telefon; digitalna forenzička analiza; forenzički alat; ekstrakcija podataka; Google podaci

SUMMARY: Smartphones are now a part of everyday life and are used for various purposes, not just for calls or messages as it was originally intended to be used. Various activities require the use of smartphones, and as a consequence of their wide application and use, a large amount of data is created. The development of forensic tools enabled the extraction of data collected by certain applications and Google Services on smartphones, such as user data, private messages, the current location of the device and visited locations of that same device. In the work, the procedure of data extraction based on Google Services was performed using the UFED Touch 2 forensic tool. The analysis of the data obtained from the extraction will be done using the Cellebrite Reader tool. The reference methodology of forensic analysis of mobile devices will be used.

KEY WORDS: Smartphone; Digital forensics analysis; forensic tools; data extraction; Google data

SADRŽAJ

1. Uvod 1

2. Primjena pametnih telefona i digitalni dokazi 3

2.1 Razvoj i upotreba pametnih telefona 3

2.1.1 Operativni sustav pametnih telefona 7

2.1.2. Android operativni sustav 8

2.2 Digitalni dokazi na pametnim telefonima 8

2.2.1 Digitalni otisak na pametnim telefonima 9

2.2.2 Pravila digitalnih dokaza 10

3. Značajke alata za forenzičku analizu uređaja i aplikacija 11

3.1. Forenzički alati za mobilnu forenziku 11

3.1.1. OpenText EnCase Forensics alat 12

3.1.2. AccessData's Forensic Toolkit FTK 12

3.1.3 Oxygen Forensic Detective alat 13

3.1.4. Autopsy alat 14

3.2 Cellebrite UFED Touch2 15

3.2.1. UFED Touch2 Ultimate 15

3.2.2. UFED Touch2 Logical 16

3.3. Forenzička analiza Android aplikacija 18

4. Google usluge primijenjene na pametnim telefonima 20

4.1. Značajke Google usluga 21

4.2. Prikupljanje i dijeljenje podataka *Google* usluga 24

5. Ekstrakcija podataka Google usluga 27

5.1. Referentna metodologija forenzičke analize mobilnih uređaja 27

5.2. Forenzičke procedure i metode ekstrakcije podataka 30

5.3. Postupak ekstrakcije Google podataka s mobilnog uređaja 32

6. Analiza prikupljenih podataka Google usluga 36

6.1 Prikupljanje i analiza podataka uređaja 38

6.2 Analiza podatkovnih datoteka u mobilnom uređaju 40

6.3 Usporedna analiza obavljenih ekstrakcija na pametnom telefonu 44

7. Zaključak 46

LITERATURA 48

Popis kratica 52

Popis slika 53

Popis tablica 54

Popis grafikona 54

1. Uvod

Pametni telefoni prate razvoj cjelokupne tehnologije i sudjeluju u istom kao odskočna daska te glavni pokretač tehnološke revolucije. Funkcionalnosti stolnih i prijenosnih računala danas su dostupne i na pametnim telefonima te se pametni telefoni danas koriste u privatne i poslovne svrhe, a koriste se i za obavljanje svakodnevnih aktivnosti i djelatnosti. Široka primjena i masovno korištenje pametnih telefona i pripadajućih aplikacija dovelo je do potrebe za generiranjem velikog broja podataka, a samim time i prikupljanja istih. Podatke mogu prikupljati aplikacije instalirane na terminalnom uređaju, web pretraživači, razne web stranice te servisi kao što su Google usluge.

Prikupljeni podaci se uz pomoć referentne metodologije digitalne forenzike mobilnih uređaja prikazuju kao digitalni dokazi. Korištenje forenzičkih alata za ekstrakciju i analizu podataka koje generiraju terminalni uređaji i aplikacije Google servisa omogućuju uvid u način korištenja terminalnih uređaja i metodologiju prikupljanja podataka.

Naslov i tema ovog diplomskog rada je Forenzika pametnog telefona temeljena na podacima Google usluga. Svrha diplomskog rada je prikazati mogućnosti i izazove primjene različitih forenzičkih alata prilikom ekstrakcije podataka i njihove analize u procesu forenzičke analize terminalnog uređaja i aplikacija. Cilj istraživanja je ekstrakcija podataka Google usluga i aplikacija korištenjem alata za forenzičku analizu i ekstrakciju te analiza ekstrahiranih podataka u forenzičkom alatu i dokumentaciju istih. Rad se sastoji od sedam poglavlja:

1. Uvod
2. Primjena pametnih telefona i digitalni dokazi
3. Značajke alata za forenzičku analizu uređaja i aplikacija
4. Google usluge primijenjene na pametnim telefonima
5. Ekstrakcija podataka Google usluga
6. Analiza prikupljenih podataka Google usluga
7. Zaključak

U drugom poglavlju je opisana primjena pametnih telefona i utjecaj razvoja terminalnih uređaja na izvođenje istrage i forenzičke analize korištenjem digitalnih dokaza te generiranje digitalnog otiska.

Značajke i raznovrsnost alata za forenzičku analizu uređaja i aplikacija te forenzička analiza na Android operativnom sustavu, zajedno s pripadajućim aplikacijama opisane su u trećem poglavlju ovog rada.

U četvrtom poglavlju objašnjene su značajke Google usluga i pripadajućih aplikacija. Prikazani su grafikoni i tablice korištenja Google aplikacija te podaci koje spremaju i prikupljaju pojedine aplikacije.

U petom poglavlju pojašnjena je referentna metodologija forenzičke analize mobilnih uređaja te je prikazana piramida metoda ekstrakcija. U ovom poglavlju je također objašnjen i postupak ekstrakcije podataka te komponente koje su se koristile.

U šestom poglavlju prikazana je analiza ekstrahiranih podataka Google usluga i aplikacija podijeljenih na podatkovne datoteke i podatke uređaja. Prikazana je usporedna analiza dobivenih rezultata za fizičku, datotečnu i logičku ekstrakciju korištenjem odgovarajućeg forenzičkog alata.

2. Primjena pametnih telefona i digitalni dokazi

Pametni telefon (engl. *Smartphone*) je terminalni uređaj sa vrlo naprednim značajkama te performansama i mogućnostima za pohranu podataka koje se razlikuju od standardnog mobilnog telefona. Najvidljivija razlika između mobilnog uređaja i pametnog telefona je zaslon osjetljiv na dodir visoke rezolucije. Ostale značajke koje posjeduju takvi uređaji su WiFi povezivost, mogućnost prihvaćanja sofisticiranih aplikacija i pregledavanja Internet sadržaja. Operativni sustavi su okosnica pametnih uređaja te oni omogućuju pokretanje i izvođenje sistemskih i ostalih aplikacija. Popularni operativni sustavi su *Android, iOS, Symbian i BlackBerry* OS, [1].

Očekivani napredak pametnih telefona nad mobilnim telefonima prikazuje se razvojem i primjenom bitnih značajki. Snažnija centralna procesorska jedinica (engl. CPU), veći prostor za pohranu, pristup Internetu, mogućnost brže i jednostavnije povezivosti, zajedno sa većim zaslonom na dodir su temeljne prednosti i razlike između pametnih telefona i standardnih mobilnih telefona. Pametni telefoni su danas opremljeni s raznim senzorima za prikupljanje informacija iz okoline te za analizu istih. Najraniji pametni telefoni imali su otporne zaslone osjetljive na dodir, koji su zahtijevali upotrebu pokazivačkih predmeta, poznatih kao olovke. Razvoj tehnike i tehnologije pokrenuo je i razvoj zaslona kakvi se koriste i danas, a koji su osjetljivi na dodir.

Pametni telefoni su dizajnirani sa softverom za ugrađene osnovne aplikacije poput kalendara, popisa kontakata, sata i vremena te sa mapama odnosno kartama. Google usluge omogućuju Android korisnicima korištenje ugrađenih osnovnih prethodno navedenih aplikacija,[2].

2.1 Razvoj i upotreba pametnih telefona

Evolucija terminalnih uređaja kao i pametnih telefona započela je sredinom devedesetih godina dvadesetog stoljeća. Prvi pametni telefon osmišljen je i izumljen 1992. godine od strane IBM (*International Business Machines*) tvrtke čije je sjedište u Sjedinjenim Američkim Državama. Dvije godine kasnije u prodaju je pušten prvi primjerak modernog pametnog telefona pod nazivom SPC (*Simon Personal Communicator).* U prvih šest mjeseci prodano je samo 50 tisuća uređaja, a cijena takvog uređaja iznosila je 900 dolara.

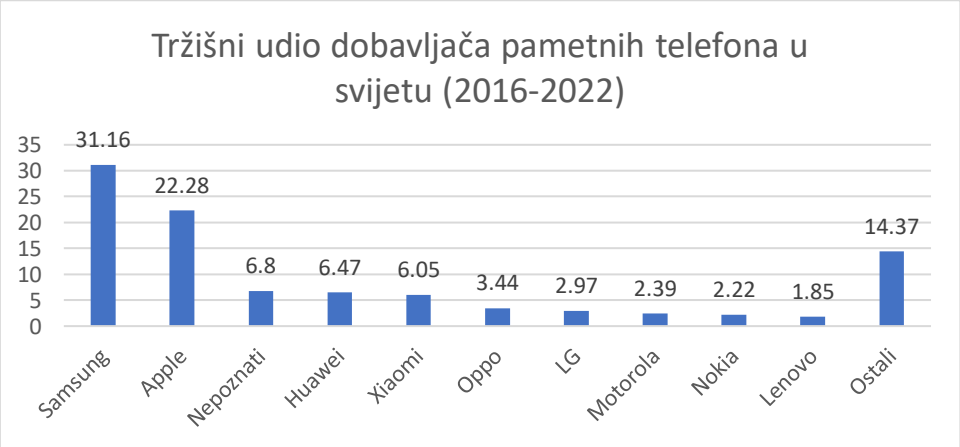
Uređaj nije bio kompaktan i elegantan kao što su to u današnje vrijeme te je imao jasne nedostatke. Vrlo težak uređaj, slab vijek trajanja baterije, mali memorijski kapacitet te nespremnost bežičnih davatelja usluga za prijenos velike količine podataka bili su razlozi nepopularnosti i slabe upotrebe u kućanstvima. Uređaj je sadržavao nekoliko bitnih elemenata, odnosno značajki koje su ga činile pametnim telefonom. Zaslon osjetljiv na dodir, mogućnost slanja i primanja e-pošte, adresar i rokovnik za sastanke, glavni su elementi koji su činili prvi pametni telefon na svijetu.

BlackBerry 850 predstavljen je 1999. godine kao osobni komunikacijski uređaj koji je uključivao sve primarne značajke uz punu *QWERTY* tipkovnicu, što je omogućilo pojednostavljeno tipkanje. Ova verzija uređaja nije uključivala mogućnost korištenja usluge poziva, ali je ta značajka ponuđena tri godine kasnije na *BlackBerry* 5810 uređaju. Nakon omogućavanja osnovnih značajki, fokus se prebacio na sigurnost i privatnost telefona te korisnika,[38].

Pojavom bežične mreže treće generacije omogućeno je pametnim telefonima povezivanje na istu te unaprjeđenje značajki, a samim time i promjenu kompletnog ekosustava i primjene terminalnih uređaja. Izgrađen je standard mobilne komunikacije koji omogućuje prijenosnim elektroničkim uređajima bežični pristup internetu, a takvi se uređaji nazivaju terminalni uređaji. Nove značajke koje su se pojavile na pametnim telefonima 2000. godine su videokonferencija i razmjena velikih privitaka e-poštom. Pojavom Steve Jobsa i *iPhone* uređaja započinje nova era terminalnih uređaja, a to je s konzumentske strane značilo kompletno korištenje Interneta na pametnom telefonu i mogućnost pretraživanja Interneta pomoću tražilica,[3],[38].

Samsung je 2010. godine ušao na tržište pametnih telefona sa *Samsung Galaxy S* uređajem, koji radi na operativnom sustavu *Android 2.1.* te posjeduje 800 x 400 Super AMOLED zaslon. Osim bržeg procesora, kao dodatna funkcionalnost pojavljuju se prednja i stražnja kamera na uređaju. Od 2010. godine do danas funkcionalnosti pametnih telefona se nadograđuju te s time i cijena uređaja raste. Pametni telefoni kakve danas poznajemo sadržavaju procesore većih brzina, više memorijskog prostora, dulje trajanje baterije te mnogo drugih unaprijeđenih karakteristika prvih pametnih telefona.

Grafikon 1. *Tržišni udio dobavljača pametnih telefona u svijetu za razdoblje 2016.-2022.*

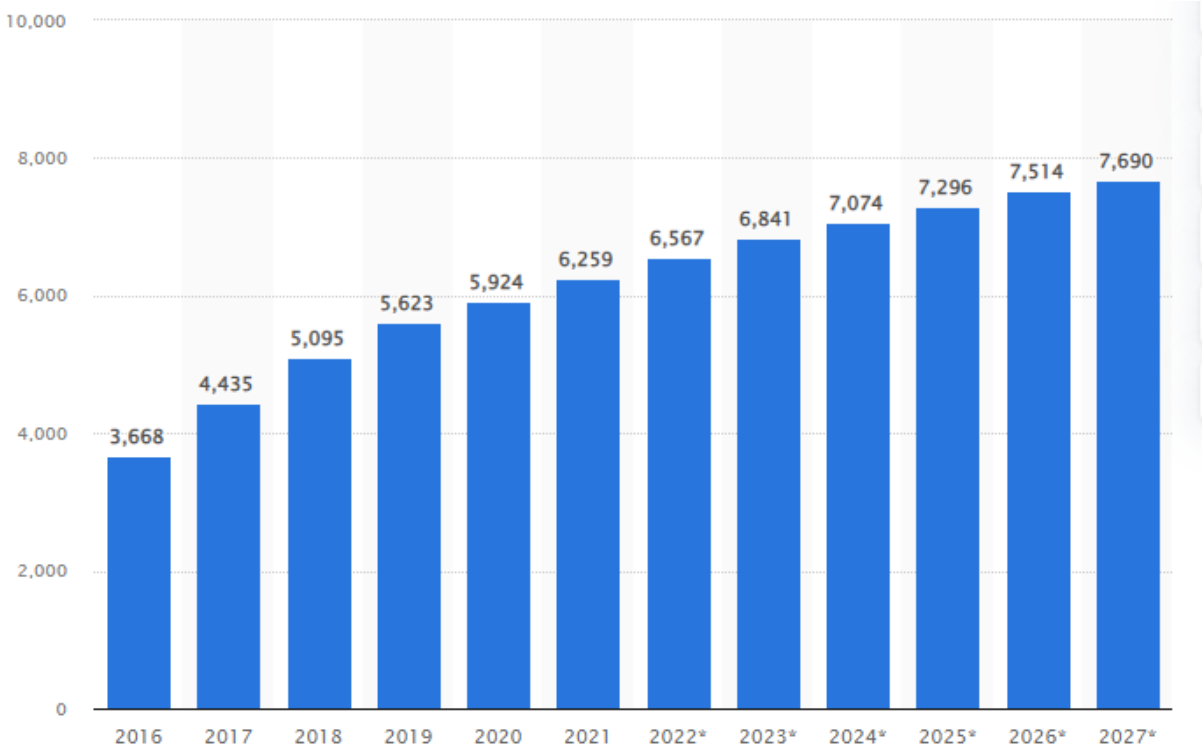


Izvor: [39]

Na grafikonu 1. prikazan je tržišni udio dobavljača pametnih telefona u razdoblju od 2016. do 2022. godine u postotcima. Najveći dio tržišnog udjela zauzimaju *Samsung* i *Apple*. Suvremeni terminalni uređaji stvorili su modernu kulturu pod nazivom „upravo sada“ koja je omogućila terminalnim uređajima pristup svjetskoj bazi podataka u nekoliko trenutaka. Ovim

postupcima podignuta su očekivanja potrošača i korisnika u smislu korištenja pametnih telefona za poslovne komunikacije i obavljanje svakodnevnih obaveza na daljinu. Poslovni prostori postali u zamjenjivi dio poslovnog ekosustava pojavom pametnih telefona, zbog mogućnosti obavljanja različitih aktivnosti i djelatnosti na dlanu korištenjem terminalnih uređaja,[4].

Broj korisnika pametnih telefona u svijetu prikazan je na y osi, dok je na osi x prikazan raspon godina (slika 1.).



***Slika 1**. Broj korisnika pametnih telefona u svijetu, [4].*

Broj korisnika u svijetu trenutno iznosi 6.5 milijardi, dok su predviđanja da će do 2027. godine broj korisnika narasti za čak milijardu korisnika i iznositi 7,6 milijardi korisnika. Broj korisnika pametnih telefona od 2016. godine do 2026. povećati će se dva puta. Procjena za 2027. godinu je, da će u cijelom svijetu 83.37% stanovništva posjedovati pametni telefon, dok će 91.16% stanovništva koristiti jednu od vrsta mobilnih telefona.

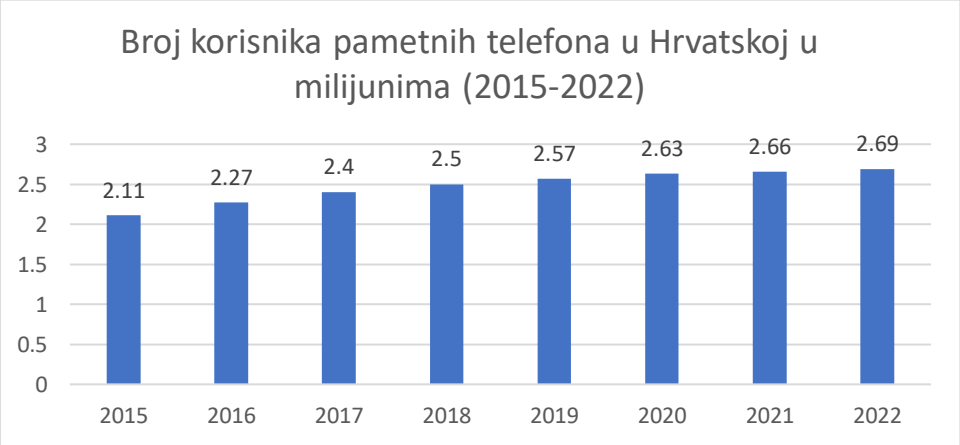
U nastavku, u tablici 1, slijedi prikaz upotrebe pametnih telefona u svijetu prema broju stanovnika u najmnogoljudnijim zemljama svijeta. Kina i Indija kao dvije najmnogoljudnije države i najveća tržišta imaju najveći broj korisnika pametnih telefona, ali im se razlikuje postotak stanovništva koje koristi pametne uređaje. U Kini 63.20% stanovništva koristi pametne telefone, dok u Indiji taj postotak iznosi 31.10%. Najveći udio korisnika pametnih telefona čine stanovnici Sjedinjenih Američkih Država s 81.6%. S druge strane Pakistan, iako ima nešto više od 220 milijuna stanovnika, pametne telefone koristi 40.59 milijuna stanovnika, što pokazuje da je udio pametnih telefona u toj zemlji samo 18.40%.

Tablica 1. *Upotreba pametnih telefona u svijetu,[40].*

Država/ tržište	Broj stanovnika	Udio pametnih telefona	Korisnici pametnih telefona
SAD	331 mil.	81.60%	270 mil.
UK	67.89 mil.	78.90%	53.58 mil.
Njemačka	83.78 mil.	77.90%	65.24 mil.
Francuska	65.27 mil.	77.60%	50.66 mil.
Južna Koreja	51.27 mil.	76.50%	39.2 mil
Italija	145.39 mil.	75.90%	45.92 mil.
Rusija	145.93 mil.	68.50%	99.93 mil.
Kina	1.44 mlrd.	63.80%	918.45 mil.
Japan	126.48 mil.	63.20%	80 mil.
Vijetnam	97.43 mil.	63.10%	61.37 mil.
Iran	83.99 mil.	62.90%	52.81. mil.
Turska	84.34. mil.	61.70%	52.06 mil.
Indonezija	273.52 mil.	58.60%	160.23. mil.
Meksiko	128.93 mil.	54.40%	70.14 mil.
Tajland	69.8 mil.	54.30%	37.88 mil.
Brazil	212.56 mil.	51.40%	109.34 mil.
Filipini	109.58 mil.	37.70%	41.31 mil.
Bangladeš	164.69 mil.	32.40%	53.3. mil.
Indija	1.38 mlrd.	31.10%	439.42 mil.
Pakistan	220.89 mil.	18.40%	40.59 mil.

Utjecaj na udio pametnih telefona u pojedinoj zemlji uvelike ovisi o ekonomskoj i društvenoj razvijenosti te platežnoj moći prosječnog stanovnika. Prema izvoru [4] i izvoru [40] predviđanja za 2022. godinu u Republici Hrvatskoj za broj korisnika pametnih telefona iznosi 2.69 milijuna korisnika, što čini 68.97% stanovništva. Na grafikonu 2 prikazano je predviđanje rasta broja korisnika u Republici Hrvatskoj od 2015. godine do 2022. godine.

Grafikon 2*. Broj korisnika pametnih telefona u Hrvatskoj u milijunima (2015-2022), [40]*

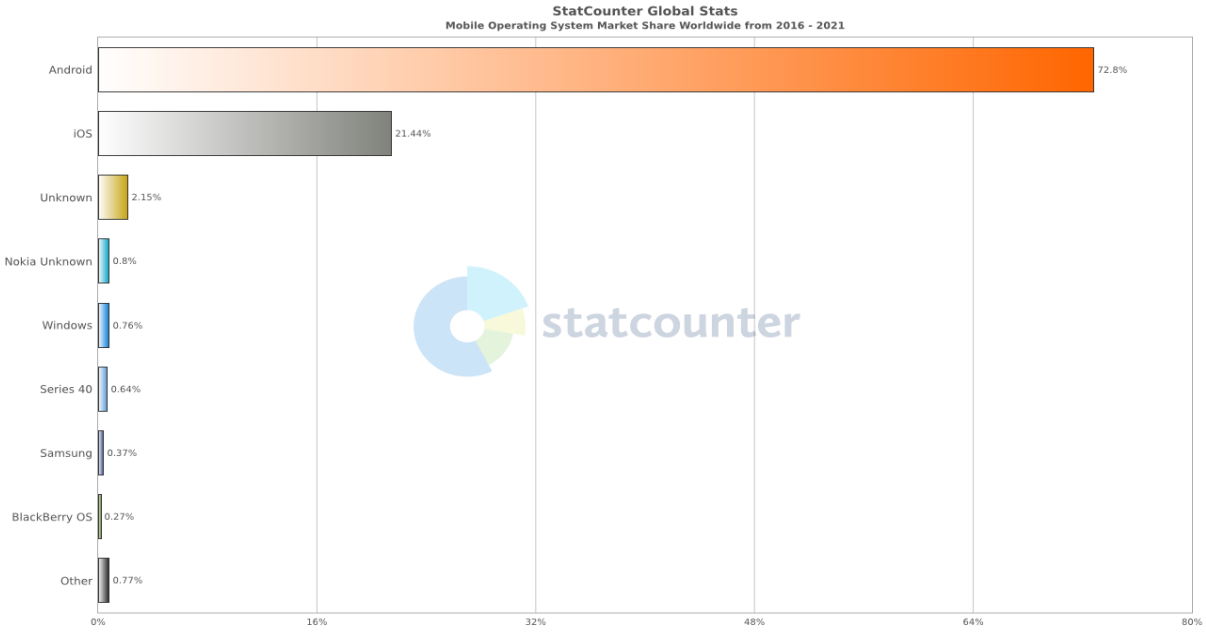


Izvor: [40]

2.1.1 Operativni sustav pametnih telefona

Operativni sustav ili OS je najbitniji softver koji se pokreće na terminalnom uređaju koji upravlja memorijom i procesima uređaja te sa svim softverskim i hardverskim komponentama. Operativni sustav je softver koji pametnim telefonima (računalima, tabletima i drugim uređajima) omogućuje pokretanje aplikacija i programa. Pokretanje OS-a izvršava se prilikom uključivanja uređaja, a mobilni operativni sustavi upravljaju povezivanjem mobilne i bežične mreže. Operativni sustavi mogu se podijeliti na zatvorene operativne sustave i na otvorene operativne sustave. Otvoreni operativni sustav je sustav otvorenog izvornog koda i može se mijenjati i prilagođavati, kao okosnica drugih otvorenih operativnih sustava. Primjer toga je *Google Android OS*.

Primjer zatvorenog operativnog sustava je *Apple* iOS. Najpoznatiji operativni sustavi su navedeni *Google Android OS*, *Apple* iOS, *KaiOS* i *Huawei Harmony OS*. Značajke koje omogućuju operativni sustavi su online trgovine koje pružaju korisnicima mogućnost pretraživanja i preuzimanja različitih vrsta aplikacija,[5].



***Slika 2**. Zastupljenost mobilnih OS-a u svijetu u periodu od 2016. do 2021. godine,[5].*

Android OS je najzastupljeniji operativni sustav ugrađen u pametne telefone u svijetu u 2021. godini. Bitnu ulogu na tržištu uz Android OS igra i *Apple* operativni sustav iOS. Zajedno čine skoro 95% tržišta u periodu od 2016. do 2020. godine, dok svi ostali operativni sustavi čine oko 5 posto tržišta u svijetu, a što je prikazano na slici 2.

2.1.2. Android operativni sustav

Android operativni sustav je mobilni operativni sustav koji je razvio *Google*, a čija je primjena primarno na terminalnim uređajima koji imaju zaslon na dodir, na pametnim telefonima i tabletima. Dizajn *Android* operativnog sustava omogućuje korisniku potpunu kontrolu i intuitivno manipuliranje mobilnim uređajem pokretima prsta na zaslonu. Osim na pametnim telefonima i tabletima, *Android* OS koristi se i na pametnim satovima, televizorima i automobilima, a glavna razlika je korisničko sučelje koje je prilagođeno ovisno o terminalnom uređaju. *Android* operativni sustav omogućio je programerima softvera i aplikacija korištenje *Android* tehnologije za razvoj mobilnih aplikacija koje se prodaju u odgovarajućim trgovinama za aplikacije, a jedna od tih aplikacija je i *Google Play*. Izvorni kod je objavljen u javnosti u formatu otvorenog koda s ciljem unaprjeđenja standarda za terminalne uređaje i pametne telefone. Pametni telefoni imaju *Android* vlasnički softver odnosno prilagođenu verziju otvorenog koda, a ne u potpunosti otvoreni kod kao što se reklamira, [6].

Rast popularnosti *Android* sustava i rivalstvo s najvećim konkurentom dovelo je do brojnih tužbi povezanih s patentima, a kao najpoznatija je tužba Oracle tvrtke. Nezakonito korištenje Java API (engl. *Application programming interface*) sučelja za razvoj vlastitog softvera dovelo je do desetogodišnjeg spora na sudu, gdje je tvrtka Oracle pokrenula tužbu protiv *Google* tvrtke za krađu i kopiranje računalnog koda. Odlučeno je u korist *Google-a* te da je kopiranje Java koda pošteno korištenje dostupnog materijala,[7].

U trećem mjesecu 2017. godine *Google* je predstavio i pustio u upotrebu verziju *Android* 8.0. poznatijom pod kodnim imenom Oreo. Ova verzija operativnog sustava dostupna je na terminalnom uređaju *Samsung Galaxy S7 Edge* koji će se koristiti u forenzičkoj analizi u diplomskom radu. Vizualne promjene u izborniku postavki, promjene u kanalima za obavijesti, sučelje za automatsko popunjavanje i bolje upravljanje lozinkama i podacima, neke su od poboljšanih značajki koje nisu bile dostupne na prethodnoj verziji 7.0. Zadnja dostupna verzija na *Android* uređajima je *Android* 12 koji je dostupan od 18. veljače 2021. godine. Jedna od važnijih značajki je poboljšano i lakše dijeljenje Wi-Fi konekcije s drugim korisnicima, a uz standardna unaprjeđenja ova verzija omogućuje dodavanje ključnih ažuriranja korištenjem *Google Play* trgovine.

2.2 Digitalni dokazi na pametnim telefonima

Značajke pametnih telefona i računala približile su se u toj mjeri, da se terminalni uređaji koriste za počinjenje kriminalnih radnji. Znanost i digitalna forenzika omogućuju otkrivanje i pronalazak dokaza na terminalnim uređajima, a pronađeni dokazi nazivaju se digitalni dokazi. Digitalni dokazi su podaci pohranjeni ili preneseni u digitalnom, odnosno binarnom obliku koji se mogu koristiti na sudu kao vjerodostojni dokazni materijal. Digitalni dokaz, kao informacija ne treba biti pohranjena u uređaju koji je ugašen ili fizički dostupan, već se takvim dokazima se može pristupiti udaljenim putem (engl. *Remote*). Takva grana digitalne forenzike se naziva

Udaljena digitalna forenzika (*Remote digital forensics)*. Digitalni dokazi se mogu nalaziti na tvrdom disku računala, kao i na pametnom telefonu. U početnoj fazi implementacije digitalni dokazi su se koristili za slučaj e-kriminala (prevare kreditnom karticom i sl.), dok se danas koriste za progon svih vrsta kaznenih djela. Datoteke pametnog telefona ili elektroničke pošte osumnjičenog mogu sadržavati ključne i kritične dokaze o namjeri, lokaciji u vrijeme zločina ili odnosu s drugim osobama,[8],[46].

Prikupljanje i analiza digitalnih dokaza te postupak računalne i mobilne forenzike sastavni su dio infrastrukture agencija za provođenje zakona. To je dovelo do potrebe za osposobljavanjem službenika za prikupljanje, razumijevanje i rukovanje digitalnim dokazima. Podaci koji se prikupljaju mogu biti statički i dinamički, a bitno ih je razlikovati zbog pristupa forenzičkoj analizi. Digitalni dokazi nastaju interakcijom sa informacijsko-komunikacijskim sustavom, a mogu se podijeliti u dvije osnovne vrste, na aktivne i pasivne digitalne dokaze.

2.2.1 Digitalni otisak na pametnim telefonima

Digitalni otisak je trag podatka koji korisnik terminalnog uređaja stvara tijekom korištenja Interneta. Svaki klik, pomak prstom na digitalnom zaslonu, stranica koja se posjećuje ostavlja digitalni trag. Također, to se odnosi i na e-poštu, datoteke i informacije te aktivnost i informacije poslane putem društvenih mreža.

Pasivni digitalni otisak ili trag je podatkovni trag koji korisnik ostavlja nenamjerno na mreži, što znači da ga sustav kreira bez znanja korisnika. Kao primjer pasivnog digitalnog otiska može se prikazati IP (engl. Internet Protocol) adresa koja služi kao identifikator pružatelja internetskih usluga i otkriva približnu lokaciju terminalnog uređaja kojeg posjeduje korisnik i povezan je nekom od mreža, a koje omogućuju pristup internetu. Iako se IP adresa mijenja i ne uključuje nikakve osobne podatke smatra se dijelom digitalnog otiska. Pasivni digitalni otisak uključuje povijest pretraživanja koje spremaju određeni web pretraživači, log zapisi, zapisi u vatrozidu, promjene i događaji u operativnom sustavu i dr.

Aktivni digitalni otisak uključuje podatke koje korisnik namjerno ostavlja ili dostavlja na mreži popunjavanjem formulara, slanjem poruka i korištenjem određenih aplikacija. Korisnik ih svjesno ostavlja na mreži interakcijom sa nekim sustavom. Slanje e-pošte je aktivan digitalni otisak zato što su podaci koji se šalju vidljivi primatelju ili više njih, a te podatke ili datoteke primatelj može preuzeti i spremiti. Takvi podaci godinama ostaju na mreži. U aktivne digitalne dokaze mogu se svrstati i prijenos fotografija i video uradaka, pohrana datoteka i fotografija te objavljivanje sadržaja na društvenim mrežama,[9].

Korištenje dostupnog sadržaja na Internetu i interakcija s IOT (enlg. *Internet of things*) sustavom iziskuje generiranje digitalnog traga, a koristi se za stvaranje profila i prilagodbu sadržaja, reklama i društvenih mreža. Uz navedeno, integritet digitalnih dokaza mora postojati i poštivati se kako bi se priznao na sudu kao relevantan i važeći dokaz.

2.2.2 Pravila digitalnih dokaza

Sve se više sudskih slučajeva odlučuje uz pomoć informacija koje se nalaze unutar mobilnih telefona, odnosno oslanjaju se na te podatke kao vitalne dokaze. Odlučujući i prevladavajući dokazi na sudu zahtijevaju dobro razumijevanje pravila dokaza te educiranost struke i sudionika u sudskom procesu. Za priznavanje dokaza na sudu potrebno je slijediti pet općih pravila dokaza koji se primjenjuju i na digitalnu forenziku, a potrebno je slijediti te dokaze kako bi bili korisni na sudu te kako slučaj ne bi bio odbačen zbog toga.

Prvo i najosnovnije pravilo koje dokazuje valjanost i važnost dokaza čine dopušteni dokazi. Potrebno je prikupiti i sačuvati dokaze na način da se mogu koristiti na sudu ili kao dokazivanje određene radnje. Potrebno je prikupiti dokaze na legalan način, inače će se takvi prikupljeni dokazi odbiti na sudu i na taj način nije moguće potvrditi kazneno djelo.

Autentični dokazi moraju biti vezani za incident i relevantni kako bi bili u skladu s zahtjevima za priznavanje na sudu. Forenzički ispitivač je osoba odgovorna za podrijetlo i autentičnost dokaza.

Prilikom prezentacije dokaza, potrebno je prikupiti sve podatke odnosno dokaze koji moraju biti jasni i cjeloviti, a takvi dokazi nazivaju se potpuni dokazi. Kako bi se održala cjelovitost i jasna slika dokaza potrebno je prikazati sve dokaze odnosno cijelu priču, a ne samo jedan dio zato što to može dovesti do pogrešnog zaključka i na koncu do drugačije presude.

Pravilo pouzdanosti dokaza govori o prikupljenim dokazima s uređaja, koji moraju biti autentični, a to ovisi o korištenim metodologijama forenzičke analize i korištenim alatima. Odabir alata za forenzičku analizu i tehnike izvođenja ne smiju dovesti u pitanje autentičnost dokaza.

Kako bi dokazi bili uvjerljivi, sudski vještak mora imati vještine i znanja procjene te mora biti u stanju objasniti na jasan i jezgrovit način postupke koji su se koristili prilikom prikupljanja dokaza. Dokazi koji su izneseni na sudu moraju biti razumljivi, jasni i uvjerljivi svim sudionicima u sudskom procesu,[10], [47].

3. Značajke alata za forenzičku analizu uređaja i aplikacija

Digitalna forenzika je grana forenzičke znanosti koja se fokusira na oporavak i istragu podataka koji se nalaze u terminalnim uređajima. Cilj forenzičke analize je oporavak i ekstrakcija podataka bez da se oni promjene. Kako je napredovala tehnologija, tako je i napredovala digitalna forenzika, a unaprjeđenje terminalnih uređaja dovelo je do potrebe za osmišljavanjem različitih metodologija i grana digitalne forenzike. Digitalna forenzika može se podijeliti na temelju vrste terminalnih uređaja koji se koriste, pa tako postoji računalna forenzika, mrežna forenzika, mobilna forenzika, cloud forenzika, forenzika baza podataka i drugi tipovi digitalne forenzike.

Mobilna forenzika je grana digitalne forenzike koja se odnosi na oporavak digitalnih dokaza s pametnih telefona i mobilnih uređaja. Načelo digitalne forenzike, pa tako i mobilne forenzike je očuvanje izvornog dokaza koji se ne smije mijenjati, iako je to vrlo teško postići u mobilnoj forenzici. Upravo zbog toga što određene podatke i konfiguraciju mobilnog uređaja tijekom forenzičke analize nije moguće očuvati u izvornom obliku, osmišljena je referentna metodologija forenzičke analize pametnih telefona i mobilnih uređaja,[10].

Alati za digitalnu forenziku sastoje je od hardvera i softvera koji se naizmjenično koriste kako bi se obavio proces digitalne forenzičke analize. Dostupni alati mogu biti komercijalni ili alati otvorenog koda, a najzastupljeniji su alati za računalnu i mobilnu forenziku. Performanse alata za provedbu forenzičke analize su vrlo visoke te zahtijevaju veći kapacitet tvrdog diska, brži CPU, veću memoriju itd. Alati za digitalnu forenziku omogućuju ekstrakciju i vraćanje obrisanih podataka s mobilnog uređaja ili računala,[48].

3.1. Forenzički alati za mobilnu forenziku

Mobilni forenzički alati služe za dohvat ili vraćanje izbrisanih datoteka i podataka, analiziranje i očuvanje dokaza koji nastaju za vrijeme procesa forenzičke analize, a mogu biti dostupni za stručnjake i istražitelje te u vlastite svrhe. Alati se mogu podijeliti na hardverski dio te na softverski dio.

Hardverski alati prvenstveno su dizajnirani za uređaje za pohranu podataka o istrazi i očuvanje integriteta dokaza na način da se ne na uređaju ne mijenjaju podaci. Forenzički kontroler diska je uređaj koji omogućuje korisniku čitanje podataka na uređaju na kojem se provodi forenzička analiza bez rizika od brisanja ili izmjene sadržaja na tom uređaju. Tvrdi disk je slikovni uređaj koji kopira sve datoteke u siguran prostor za pohranu. Hardverski alati se sastoje i od uređaja za oporavak lozinke koji koriste algoritme, kao što su *brute-force* algoritmi za otkrivanje lozinke na zaštićenom uređaju.

Karakteristike softverskih alata i aplikacija jesu višenamjensko korištenje, odnosno mogućnost izvršavanja više zadataka u isto vrijeme i u jednom korištenju. Mogućnost takvih

alata je obrada različitih uređaja ili upravljanje različitim operativnim sustavima istodobno kao što su *Windows* i *Linux*. Osim pametnih telefona i mobilnih uređaja, softverskim alatima mogu se ispitati uređaji kao što su tableti i pametni satovi te pripadajuće aplikacije. Alati za mobilnu forenziku mogu se podijeliti prema operativnom sustavu na pametnom telefonu, a najpoznatiji su *iOS* i *Android*,[11].

3.1.1. OpenText EnCase Forensics alat

OpenText EnCase je moćno i jedno od najpovjerljivijih rješenja za mobilnu forenziku. Softver koji se koristi u ovom slučaju izgrađen je s dubokim razumijevanjem metodologije za mobilnu forenziku i za 6 osnovnih faza digitalne istrage. Ugrađena su dva tijeka rada koja uključuju kompletno istraživanje i razvrstavanje, odnosno trijažu. Prvi radni tijek omogućuje temeljito ispitivanje, dok drugi omogućuje ispitivaču jednostavno i brzo dodavanje dokaza. Ovaj alat omogućuje pronalazak nepoznatih podataka i datoteka u datotečnom sustavu, a istovremeno održava integritet dokaza pohranjivanjem formata spisa prihvaćenog na sudu. Također, nudi i mehanizme obrade velike brzine i optimizirane performanse te podršku za operativne sustave. Omogućuje profesionalna, ali istovremeno i lako čitljiva izvješća koja se mogu stvoriti putem prilagodljivih predložaka. Najveća prednost ovog alata je omogućavanje ispitivaču neometano dovršavanje bilo koje pokrenute istrage. Dostupan je za korištenje na najnovijim pametnim telefonima, tabletima, GPS (engl. *Global Positioning System*) uređajima i pametnim satovima.

3.1.2. AccessData's Forensic Toolkit FTK

AccessData Toolkit FTK je napredni alat za mobilnu forenziku koji nudi kombinaciju brzine, stabilnosti, snage, tehnologije i brzog pretraživanja s jednim samostalnim softverom. FTK alat omogućuje istražiteljima pristup za ekstrakciju i analizu mobilnih uređaja i pametnih telefona korištenjem tehnologije e-otkrivanja. Glavna značajka ovog alata je postojanje dijeljene indeks datoteke koja se koristi za brzo filtriranje i pretraživanje, odnosno eliminira se potreba za čekanjem i dovršavanjem pretraživanja, a samim time i eliminira se potreba za dupliciranjem datoteka. Neovisno s kojom se količinom podataka radi, FTK koristi sto posto svojih hardverskih resursa za najbrže pronalaženje relevantnih dokaza. Napredni alat, kao što je FTK, koristi bazu podataka s jednim dijeljenjem koja sigurno sprema sve podatke, a to sprječava složenost i smanjuje cijenu. Podrška za timski rad bez prekida i onemogućavanje gubitaka već ekstrahiranih podataka tijekom rušenja GUI-a (*graphical user interface*) povezne su značajke koje daju prednost FTK alatu u odnosu na druge alate za mobilnu forenziku.

Ovaj alat nudi mogućnost kreiranja kriterija i prema određenim specifikacijama smanjivanje nevažnih i manje krucijalnih podataka, kao što su vrsta podataka, veličina datoteka te veličina piksela. Kompletnu ekstrakciju, oporavak podataka i obradu istih omogućuje čarobnjak koji osigurava arhiviranje svih kritičnih podataka. Usporedba značajki forenzičkih alata AccessData FTK i *EnCase Forensic* prikazana je u tablici 2. FTK alat ne podržava procese naredbenog retka (engl. *Command-line process*), dok *EnCase Forensic* ima mogućnost procesuiranja naredbi,[12],[49]

***Tablica 2**. Usporedba značajki forenzičkih alata, [42]*

Značajke alata	AccessData FTK	EnCase Forensic
Akvizicija		
Logička kopija podataka	DA	DA
Fizička kopija podataka	DA	NE
Datotečna akvizicija	DA	DA
GUI	DA	DA
Procesi naredbenog retka	NE	DA
Udaljeni pristup/akvizicija	DA	DA
Ekstrakcija		
Pregled datoteka	DA	DA
Pretraživanje ključnih riječi	DA	DA
Dekompresija	NE	DA
Dekriptiranje	DA	NE
Označavanje	DA	DA
Izvještavanje		
Log izvještaji	DA	DA
Vremenska crta	DA	DA
Generator izvještaja	DA	DA
Označavanje	DA	DA

Prilikom ekstrakcije podataka *EnCase Forensic* alat ne nudi mogućnost dekriptiranja podataka i datoteka. FTK alat ne nudi dekompresiju podataka, pa je potrebno za potpunu akviziciju podataka koristiti oba forenzička alata ili pronaći alat koji nudi sve te mogućnosti.

3.1.3 Oxygen Forensic Detective alat

Oxygen Forensic Detective je cjelovita forenzička softverska platforma izgrađena za ekstrakciju, dekodiranje i analizu podataka iz širokog spektra digitalnih izvora kao što su pametni telefoni, mobilni uređaji, IoT uređaji, dronovi i *cloud* usluge. Svjetski je lider u ekstrakciji podataka s cloud platformi sa *SecMail, iCloud, Google, WhatsApp* i drugim liderima.

Ekstrakcija podataka i datoteka s *Android* uređaja, *iPhone* uređaja te ostalih mobilnih uređaja, pa čak i ekstrakcija povijesti leta omogućena je korištenjem ovog alata za mobilnu ekstrakciju. Vjerodajnice i korisnički podaci se mogu prikupljati s računala, dok se vitalni dokazi izvlače iz IoT uređaja, nosivih uređaja i memorijskih kartica. *Forensic Oxygen* omogućuje istražiteljima i ispitivačima generiranje i izvoz izvješća u različite formate koji uključuju PDF, XML, XLS i RTF. Korištenjem USB (engl. *Universal Serial Bus*) *Dongle* komponente istražitelj može kroz jedno sučelje istraživati više slučajeva i vršiti više ekstrakcija istovremeno. Alat sadrži značajku pretraživanja što znatno olakšava proces uvoza sigurnosnih kopija. Mogu se pretraživati po ključnoj riječi, skupu podataka i drugim proizvoljnim kriterijima.

Posljednja verzija *Oxygen Forensic Detective* alata koristi najnoviju metodu ekstrakcije podataka s aplikacije *Signal*, koja se naziva *Oxi agent* i omogućuje fizičku ekstrakciju, zaobilaženje lozinki na zaslonu telefona korištenjem više multimedijskih uređaja ili *Qualcomm* elektroničkih komponenti,[12],[13].

3.1.4. Autopsy alat

Autopsy je pouzdana i jednostavna za korištenje platforma za digitalnu, odnosno mobilnu forenziku koju koriste vojska, službe za provođenje zakona te korporativni ispitivači. Karakteristike ovog alata su dostupnost i mogućnost preuzimanja bez naplate za svakog korisnika. Sučelje alata jednostavno je za korištenje i nakon instalacije omogućeno je usmjeravanje korak po korak, što dovodi do lakog upravljanja sa zadacima. Kao i prethodni alat, *Autopsy* je zasnovan na GUI-u koji učinkovito procjenjuje pametne telefone i tvrde diskove računala. Također, posjeduje podršku za Android uređaje, a omogućuje ekstrakciju kontakata, zapisnika poziva, poruka i podataka pojedinih aplikacija. *Autopsy* služi kao digitalna forenzička platforma i grafičko sučelje primarno za *The Sleuth Kit* te druge forenzičke alate.

Ovaj forenzički alat dolazi s *plug-In* arhitekturom i platformom koja omogućuje uporabu modula, kao što su analiza vremenske trake, filtriranje hash memorije i pretraživanja ključnih riječi. Zadaci koje zahtijevaju istražitelji odvijaju se istovremeno i paralelno iz više jezgri, dok istražitelj vrši ekstrakciju ili analizu nekog uređaja, a produkt toga je brzo pružanje rezultata istrage. *Autopsy* alat uključuje sve temeljne značajke koje posjeduju ostali forenzički alati, a najveća prednost ovog alata je isplativost korištenja, zato što je ovaj alat besplatan. Glavne karakteristike *Autopsy* forenzičkog alata su:

1. Jednostavna instalacija na *Windows OS*
2. Automatizirani i intuitivni tijek rada
3. Mogućnost ekstrakcije artefakata iz Internet pretraživača
4. Koristi MD5 (engl. *Message-digest*) Hash za verifikaciju integriteta datoteka i podataka
5. Indeksirano pretraživanje ključnih riječi
6. Vremenska analiza svih događaja unutar uređaja
7. Galerija slika za pregledavanje

Usporedba forenzičkih alata za analizu podataka prema integritetu podataka, prikupljanju podataka, analizi podataka te formatu izvještaja prikazana je u tablici 3.

***Tablica 3**. Značajke forenzičkih alata za analizu podataka,[42],[43]*

Značajke	Forenzički alati		
	Oxygen Forensic Suite	Cellebrite UFED Logical Analyzer	Autopsy The Sleuth Kit
Integritet podataka			
MD-5	DA	DA	DA
SHA-1	DA	DA	DA
SHA-256	DA	NE	NE
Prikupljanje podataka			
Logičke datoteke	DA	DA	DA
Memorijska kartica	NE	NE	DA
Fizička ekstrakcija	NE	NE	NE
Formati izvještaja			
CSV	DA	DA	NE
PDF	DA	DA	DA
TXT	NE	NE	DA
XML	DA	DA	DA
HTML	DA	DA	DA
Analiza podataka			
Označavanje	DA	NE	DA
Tekstualni preglednik	DA	NE	DA
Hex preglednik	DA	NE	DA
Sortiranje podataka	DA	NE	DA
Oporavak podataka	DA	DA	DA
Usporedba podataka	NE	NE	DA

3.2 Cellebrite UFED Touch2

UFED Touch (engl. *Universal Forensic Extraction Device*) je univerzalni uređaj za forenzičku ekstrakciju, nova generacija mobilnih forenzičkih rješenja koja omogućuje tehnološki najnapredniju ekstrakciju, dekodiranje, analizu i izvještaj o podacima u pametnim telefonima i mobilnim uređajima. *UFED Touch 2* može izvoditi četiri vrste ekstrakcije svih podataka iz najšireg raspona uređaja, čak i ako su podaci izbrisani. *UFED Touch* izvodi fizičku ekstrakciju, logičku ekstrakciju, datotečnu ekstrakciju i ekstrakciju lozinke.

Mobilni uređaji, pametni telefoni, prijenosni GPS uređaji, tableti i telefoni proizvedeni s kineskim čipsetima, odnosno njihovi podaci mogu se ekstrahirati i analizirati *UFED Touch 2* alatom. Ovaj alat se sastoji od vlastitog hardvera, integrirane baterije GUI zaslona osjetljivog na dodir koji ubrzavaju postupak istrage.

3.2.1. UFED Touch2 Ultimate

UFED Touch Ultimate rješenje može se podijeliti u 3 napredne aplikacije koje ubrzavaju istragu i pojednostavljuju postupak:

1. UFED *Physical Analyzer* – napredna aplikacija za dekodiranje, analizu i izvještaj
2. UFED *Phone Detective* – aplikacija za trenutno detektiranje mobilnog telefona
3. UFED *Reader* – aplikacija koja omogućuje ovlaštenim ispitivačima dijeljenje informacija s drugim osobama,[15]

Karakteristika ovog alata je pružanje ispitivačima maksimalne mogućnosti za ekstrakciju i analizu mobilnih uređaja. Prednosti koje posjeduje *UFED Touch 2 Ultimate* alat su:

1. Mogućnost fizičke ekstrakcije s *BlackBerry* uređaja koje pokreće OS 4-7 i dekodiranje podataka, aplikacija e-pošte i drugih aplikacija
2. Najširа podrška za *Apple* uređaje s operativnim sustavom iOS 3 i novije verzije
3. Fizička ekstrakcija i dekodiranje lozinki i pinova zaobilaženjem s *Android* uređaja
4. Najmoćnije rješenje za telefone s kineskim čipset-ima
5. Dohvaćanje postojećih i izbrisanih podataka s aplikacija uređaja
6. Česta ažuriranja koja osiguravaju kompatibilnost s novim pametnim telefonima koji se pojavljuju na tržištu.

***Slika 3**. UFED Touch2 Ultimate komplet,[16]*

Na slici 3. prikazan je *UFED Touch 2* komplet, koji se sastoji od *UFED Touch 2* uređaja, kofera te pripadajućih pretinaca s potrebnom opremom za ekstrakciju i prepoznavanje uređaja.

3.2.2. UFED Touch2 Logical

UFED Touch 2 Logical je rješenje za mobilnu forenziku za brzu i logičku ekstrakciju podataka iz pametnih telefona, mobilnih telefona, GPS uređaja i tableta. Ovaj alat koristi intuitivno grafičko sučelje s jednostavnim zaslonom na dodir koje pruža forenzičke dokaze u stvarnom vremenu i pohranjuje ih. Kao i Ultimate verzija *UFED Touch 2* uključuje tri aplikacije :

1. *UFED Logical Analyzer*
2. *UFED Phone Detective*
3. *UFED Reader*

Napredne istraživačke mogućnosti koje pruža ovaj alat su:

1. Logička ekstrakcija podataka širokog spektra mobilnih uređaja i pripadajućih operativnih sustava (*BlackBerry, iOS, Android, Nokia, Symbian, Windows Phone*)
2. Kloniranje SIM ID-a koje neutralizira uređaj od bilo kakve mreže aktivnosti tijekom analize, a istovremeno zaobilazi lozinke, pinove i zaključane SIM kartice
3. Česta ažuriranja kako bi se osigurala kompatibilnost s novim pametnim telefonima na tržištu
4. Analiza, generiranje izvještaja i prilagodba pomoću UFED logičkog analizatora
5. Modul jednostavan za upotrebu gdje nije potrebno računalo za ekstrakciju
6. Potpuno opremljen forenzički komplet sa svim elementima potrebnim za istragu, [17].

***Slika 4**. UFED Touch2 radna jedinica, [18]*

Na slici 4. prikazana je radna jedinica *UFED Touch 2* forenzičkog alata koji omogućuje udaljeni pristup i korištenje na terenu. Usporedba funkcionalnosti *UFED Touch* 2 alata za digitalnu forenziku prikazan je u tablici 4. Iz tablice je vidljivo kako *Ultimate* inačica forenzičkog alata podržava sve vrste ekstrakcije, dok se datotečna i fizička ekstrakcija ne mogu obaviti s *Logical* inačicom. Sve *UFED Touch 2* verzije podržavaju ekstrakciju više od 4000 različitih uređaja.

***Tablica 4**. Usporedba funkcionalnosti UFED Touch 2 alata,[31]*

Funkcionalnosti	Cellebrite UFED Touch Ultimate	Cellebrite UFED Touch Logical
Fizička ekstrakcija	DA	NE
Logička ekstrakcija	DA	DA
Datotečna ekstrakcija	DA	NE
Ekstrakcija podataka SIM kartice	DA	DA
Ekstrakcija zaporke	DA	DA
Kloniranje SIM kartice	DA	DA
Ekstrakcija snimki zaslona/ fotografija	DA	Opcionalno

3.3. Forenzička analiza Android aplikacija

Forenzička analiza aplikacija je kompleksni sustav koji se može prikazati kao posebna znanost, a opisuje se kao umjetnost u kojoj postoji bezbroj načina pohrane i prikrivanja podataka. Kompleksnost ovakvog ekosustava dokazuju različite verzije aplikacija koje mogu na različiti način pohranjivati iste podatke. Ovakve okolnosti otežavaju i ograničavaju ispitivačima postupak forenzičke analize. Različiti načini pohrane podataka dovode do problema koji uključuje različite metode za ekstrakciju i pohranu podataka. Metode koje se uzimaju u obziru mogu biti relevantne jedan dan, dok drugi dan ta ista metoda ili više njih prestaje biti relevantna i ne može se koristiti. Cilj forenzičke analize aplikacija je razumijevanje korištenja aplikacije i pronalazak korisničkih podataka.

Android aplikacije na pametnim telefonima su instalirane unaprijed te se nazivaju sistemske aplikacije. Karakteristika ovih aplikacija je onemogućavanje korisniku brisanje tih aplikacija. Prilikom pripreme pametnog uređaja, prije ekstrakcije i analize ispitivač ne može znati pozadinu sistemskih aplikacija odnosno koje potencijalno korisne podatke sadrži pojedina aplikacija. Kompliciranа izvedba forenzičke analize može dovesti ispitivača u iskušenje da preskoči određene aplikacije, za koje se smatra da sadrže mali broj podataka i informacija, kao što su *Gaming* igre. Ovakav primjer aplikacija posjeduje ugrađenu značajku za razmjenu poruka, koje su izvor informacija i mogu biti korisne u forenzičkoj istrazi, odnosno aplikacije za razmjenu poruka najvrjedniji su izvor podataka i informacija.

Aplikacije kao što su kontakti i pozivi sadrže log file-ove ili dnevnike podataka te se oni pohranjuju u istoj bazi podataka. Kontakti ne trebaju biti uvezeni ili dodani od strane korisnika, već mogu biti automatski generirani od strane *Google* usluga, kao što su *Gmail* i *Google Disk*,[19].

***Slika 5**. Datoteke i podaci Android aplikacija,[19].*

Na slici 5. prikazani su nazivi paketa, te datoteke na koje je potrebno obratiti pažnju prilikom forenzičke analize aplikacija za kontakte i pozive.

Google Chrome pretraživač je osnovni pretraživač velike većine pametnih uređaja. *Chrome* podaci koji se nalaze na uređajima su specifični i jedinstveni zato što sadrže podatke i informacije sa svih uređaja na kojima se korisnik prijavio s istim profilom. Podaci pronađeni forenzičkom analizom aplikacije, odnosno podaci pronađeni u bazi podataka pametnog uređaja mogu biti podaci koji su generirani na računalu, tabletu ili nekom trećem uređaju.

Package name: com.android.chrome

Files of interest:

- /app_chrome/Default/:
  - Sync Data/SyncData.sqlite3
  - Bookmarks
  - Cookies
  - Google Profile Picture.png
  - History
  - Login Data
  - Preferences
  - Top Sites
  - Web Data
- /app_ChromeDocumentActivity/

***Slika 6**. Google Chrome podatci,[19].*

Google Chrome podaci koji se zapisuju i koji se mogu ekstrahirati te analizirati prikazani su na slici 6. Analiza aplikacija za razmjenu poruka, poziva i video poziva, kao što su *WhatsApp, Facebook Messenger, Skype i Signal* sastoji se od ekstrakcije više slojeva podataka. Podaci koji se mogu ekstrahirati i analizirati mogu biti podaci pohranjeni u memoriji na pametnom uređaju ili podaci pohranjeni na SD (Secure Digital) kartici. Pojedine aplikacije automatski spremaju podatke, kao što su fotografije, dokumenti i videozapisi na prvo slobodno mjesto u memorijskom djelu, ovisno o kapacitetu memorije na pametnom telefonu i SD kartici.

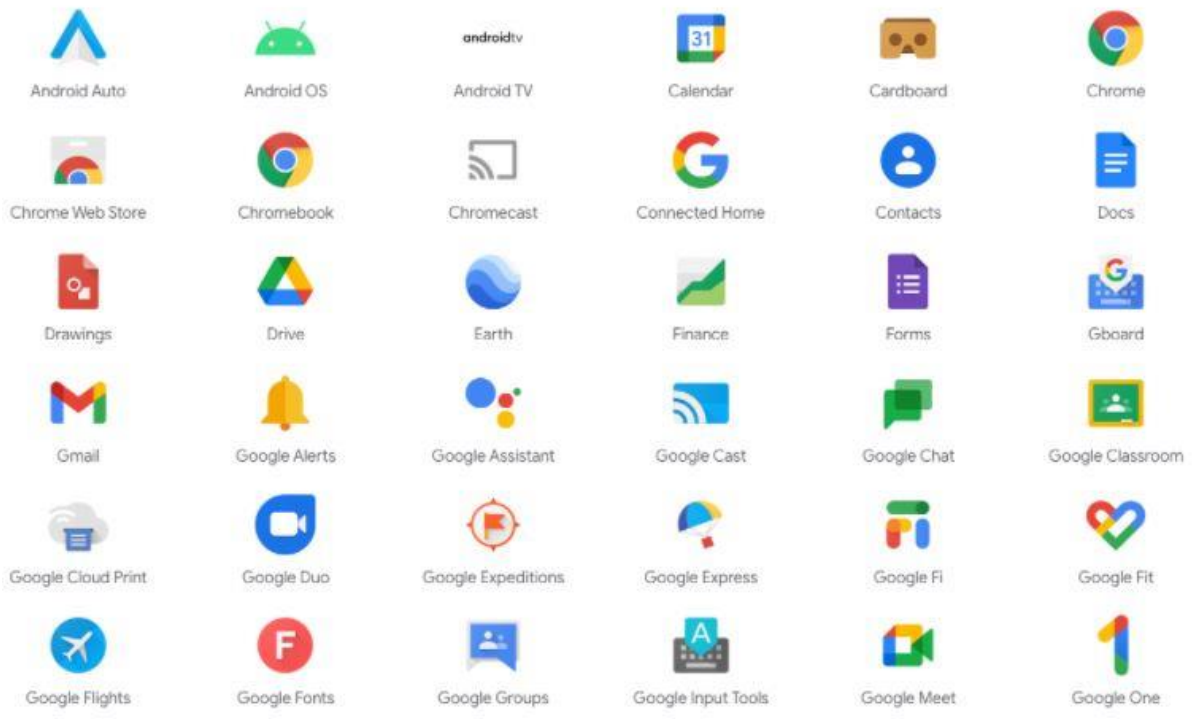
Ovakav tip aplikacija koristi enkripciju podataka kako bi se zaštitila privatnost poruke te je potrebno koristiti alate za dešifriranje tih podataka. Ovisno o vrsti aplikacije potrebno je koristiti različite metode i različite alate za dešifriranje podataka i sigurnosnih kopija,[19].

4. Google usluge primijenjene na pametnim telefonima

Google LLC je američka multinacionalna korporacija specijalizirana za mrežne usluge i proizvode. *Google* usluge mogu biti mobilne, računalne i kompatibilne sa svim uređajima. Svojstvo *Google* usluga je povezivost, koja omogućuje povezivanje jednog računa na više različitih uređaja. Glavna misija *Google* tvrtke je organizacija informacija dostupnih u svijetu i omogućiti globalnu dostupnost i korisnost istih. Glavne karakteristike *Google* usluga i odgovor na pitanje zašto koristiti te usluge su:

1. Pouzdanost i sigurnost
2. *One Pass* značajka
3. Velik broj dostupnih usluga

Google usluge su na vrhu ljestvice najsigurnijih i najpouzdanijih Internet usluga dostupnih u svijetu tehnologije i IoT-a. *One Pass* je jedna od najboljih značajki *Googleovih* usluga koja omogućuje korištenje svih *Googleovih* usluga i zaštitu istih s jednom lozinkom. Ova značajka dopušta i omogućuje pristup svim povezanim uslugama korištenjem samo jedne lozinke. Velik broj dostupnih usluga koje nudi *Google* imaju jedan uvjet za korištenje, a to je internetska veza.



***Slika 7**. Dio dostupnih Google usluga,[20]*

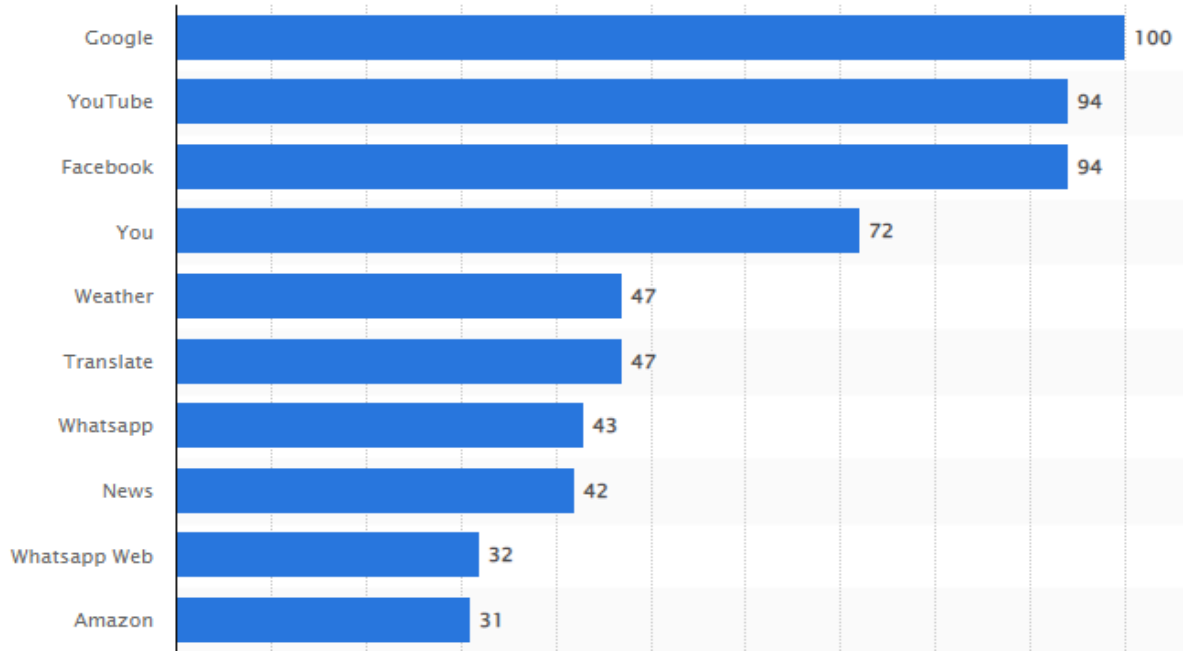
Na slici 7. prikazan je dio spektra usluga koje su dostupne, a ukupan broj usluga koje pripadaju *Google* uslugama je 271. Usluge se mogu podijeliti na standardne usluge i cloud usluge ovisno o načinu korištenja i pohrane podataka,[20]

4.1. Značajke Google usluga

Pojedine dostupne usluge tvrtke *Google* mogu se koristiti na *Android* uređajima. Aplikacije kao što su pretraživač, kalendar, mail, *cloud* pohrana i *Google* karte su dostupne unaprijed na terminalnim uređajima, odnosno instalirane su na uređaj u trenutku prije nego što su pametni telefoni dostupni korisnicima. *Google* pretraživač i *Google Play* usluga su dvije početne i najvažnije *Google* usluge dostupne na pametnim telefonima.

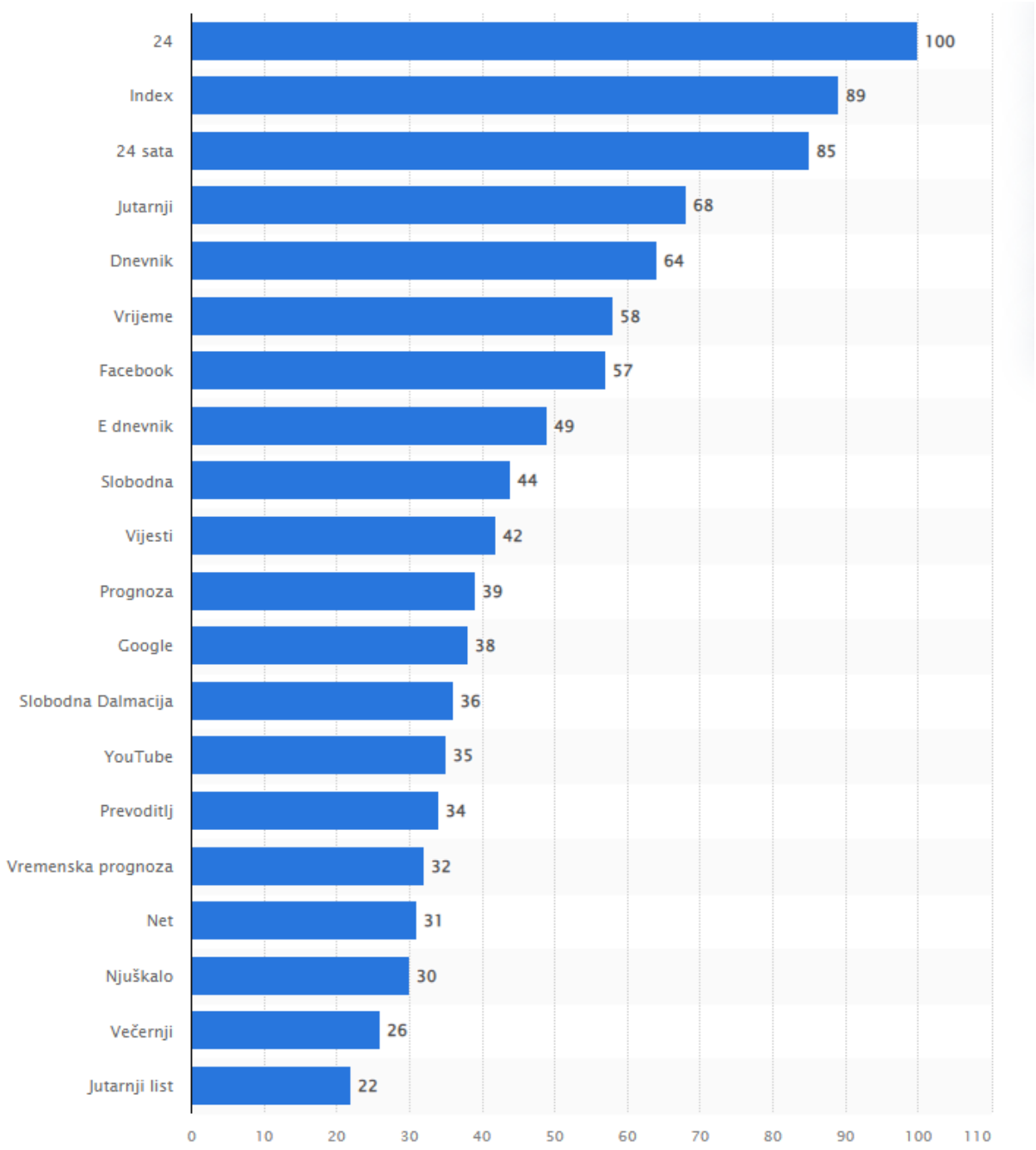
Prema *Alexa* statistici prometa *Google* usluga i proizvoda najpopularniji proizvodi su: *Google* tražilica, mail, dokumenti, karte, prevoditelj, vijesti te trgovina *Play*, a više od milijardu korisnika koristi jednu ili više usluga i proizvoda.

Google tražilica ili pretraživač *(google.com)* je najpopularnija i najčešće korištena tražilica u svijetu. *Google* zauzima više od 70 posto tržišnog udjela svih dostupnih tražilica. Većinu prometa koji se generira te promet koji imaju web stranice dolazi od *Google-a*. *Google* tražilica prosječno obrađuje više od 40 tisuća upita ili pretraživanja svake sekunde, a najtraženiji pojam je *Google*.[21].



***Slika 8**. Najtraženiji pojmovi u 2021.godini, [22]*

Google Chrome je Internet preglednik koji nudi sigurnost, brzinu i stabilnost za vrijeme korištenja i pregledavanja na mreži. Na slici 8. prikazani su najtraženiji pojmovi u *Google* tražilici u svijetu za 2021. godinu prema Indeks vrijednosti. Preglednik omogućuje veću produktivnost korištenjem ostalih aplikacija koje nudi *Google* i integraciju za rad izvan mreže s aplikacijama kao što su *Gmail* i Dokumenti. Korištenjem navedenih aplikacija u pregledniku moguće je nastaviti s radom i bez pristupa internetu. Glavna značajka preglednika je sinkronizacija podataka, spremljenih zaporki i oznaka koja omogućuje pristup na ostalim terminalnim uređajima.



Slika 9. *Najtraženiji pojmovi na Google tražilici u Republici Hrvatskoj prema indeks vrijednosti, [44].*

Najtraženiji pojmovi u siječnju 2020. godine u Republici Hrvatskoj prema indeks vrijednosti prikazani su na slici 9. U Republici Hrvatskoj najviše pretraživanja imaju najpopularniji novinski portali. Zanimljivost je, da je u ključna riječ *Google* na 12. mjestu pretraživanja u tražilici pod istim imenom. Uz *Google* na listi top 20 ključnih riječi je *YouTube,* koji se nalazi dva mjesta ispod.

Gmail je sigurna i pametna e-pošta koja je integrirana s *Google* aplikacijama i proizvodima za jednostavniju upotrebu koju koristi više od 1.8 milijardi korisnika. Stvara uvijete korisniku za potpunu kontrolu i iskustvo. Koristi se više razina sigurnosti i najnaprednija zaštita protiv krađe identiteta. *Gmail* je dio *Google Workspacea*, odnosno skupa alata za produktivnost i

suradnju koji pomažu tvrtkama, timovima i pojedincima praćenje svakog detalja. Uz *Gmail* skup alata čine Kalendar, Disk, Dokumenti, Tablice i druge povezane aplikacije.

Google Kalendar služi za jednostavnu organizaciju rasporeda i događaja. Povezan je s *Gmail* aplikacijom, pa se događaji automatski dodaju u kalendar. Dodatna značajka kalendara je pohranjivanje događaja i rasporeda na internetu.

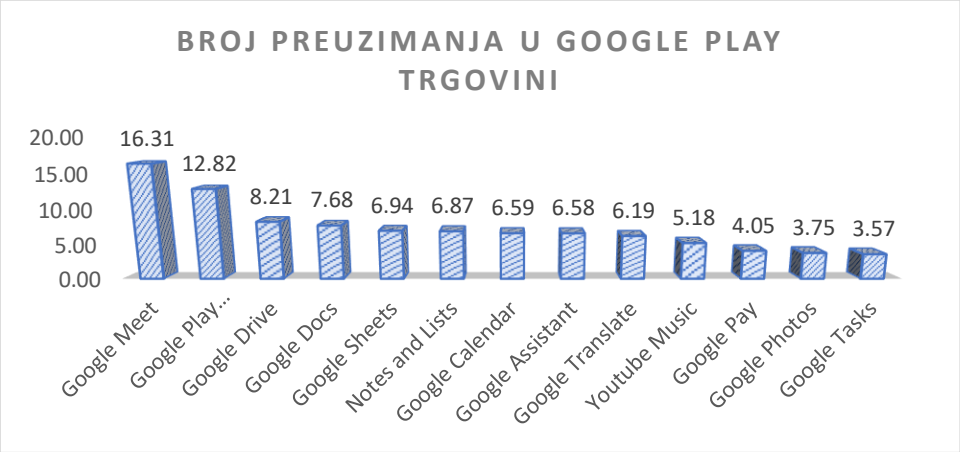
Google Dokumenti su skup alata za pametno uređivanje i dodavanje stilova te za jednostavno oblikovanje teksta i odlomaka. Glavna značajka aplikacije je pristupanje te izrada i uređivanje dokumenata putem različitih terminalni uređaja. *Google* datoteke su funkcionalne s word programom, a omogućeno je i formatiranje datoteka. Uz tablice, prezentacije i obrasce čini kvartet aplikacija koje uspješno zamjenjuju *Office* programe za jednaku namjenu.

Google Disk je *cloud* rješenje za jednostavan i siguran (šifriran) pristup cjelokupnom korisničkom sadržaju. Pohrana i dijeljenje datoteka glavne su značajke Diska. *Google* jamči sigurnost i privatnost sadržaja te nekorištenje istog za prilagodbu oglasa. *Google* Disk je integriran s ostalim aplikacijama u oblaku i alatima te omogućuje suradnju u stvarnom vremenu.

Google Play usluga je najvažnija komponenta i aplikacija *Google-ovih* proizvoda koja omogućuje i pokreće aplikacije u pozadini mobilnih terminalnih uređaja na *Android* operativnim sustavima od verzije 2.2. do najnovije verzije. Dvije najvažnije sigurnosne značajke su verifikacija aplikacija i zaštita aplikacija (*SafetyNet)*,[23].

Google Play Trgovina je mjesto za preuzimanje i kupovanje milijuna aplikacija, igara i ostalih medija, kao što su filmovi, serije, podcasti na *Android* terminalne uređaje. *Google Play* usluga omogućuje aplikacijama i aplikacijama trećih strana razmjenu informacija s *Google-om*, a Trgovina korisnicima pruža mogućnost korištenja aplikacija i njihovu dostupnost. Broj preuzimanja najpopularnijih *Google* aplikacija u *Google Play* Trgovini za 6. mjesec 2021. godine prikazan je na grafikonu 3.

***Grafikon 3**. Broj preuzimanja aplikacija u 6. mjesecu 2021. godine u milijunima*



Izvor: [22]

4.2. Prikupljanje i dijeljenje podataka *Google* usluga

Google prikuplja podatke kako bi personalizirao i prilagodio proizvode i usluge za svakodnevno korištenje, odnosno prikuplja podatke o tome kako korisnik koristi aplikacije, usluge i uređaje. To prikupljanje podataka služi za praćenje online navika i preferencija korisnika. Odgovorno postupanje s podacima i zaštita korisničkih podataka regulirana je u *Google* pravilima privatnosti. Prema korisnikovom digitalnom zapisu *Google* stvara digitalni profil korisnika korištenjem ciljanog oglašavanja, praćenja lokacije, poboljšanja upotrebljivosti, algoritama za podešavanje i uočavanje trendova i analiza.

Različite tehnologije za praćenje weba koje koristi *Google* su praćenje IP adrese koja služi za identifikaciju korisničke lokacije odnosno lokacije terminalnog uređaja ili računala te rad s kolačićima (engl. Cookies). Mali isječci koda pohranjuju se u preglednik kod prvog posjeta web stranici, a pomažu različitim web stranicama da zapamte i identificiraju promet koji je korisnik generirao na toj istoj web stranici.

Vrste korisničkih podataka koje *Google* prikuplja su:

1. Jezik ili jezici kojima korisnik govori
2. Mjesta koja korisnik traži i posjećuje na *Google* kartama
3. Stvari koje korisnik kupuje i proračun za potrošnju
4. Omiljene trgovine
5. E-poštu, privitke, neželjenu poštu i izbrisane datoteke i mailove
6. Podatci spremljeni na Disku
7. Navike gledanja na *YouTube* platformi, komentari i svi pogledani videozapisi
8. Raspored u kalendaru i planovi
9. Članci koji su pročitani na *Google* vijestima
10. Oglasi koji su pregledani i aplikacije koje se koriste,[24].

Prosječni Android uređaj šalje podatke *Google-u* čak i kad je neaktivan, a za vremenski period od 12 sati šalje se 1 MB podataka. Za isti vremenski period neaktivnosti iOS uređaj šalje *Apple-u* 52 KB podataka. Prema *Google* pravilima privatnosti prikuplja se samo sadržaj koji korisnik stvara, koristi, prenosi ili prima za vrijeme korištenja usluga i aplikacija. Prema načinu pristupanja *Google* uslugama postoje četiri kategorije pristupanja i prikupljanja podataka:

- Aplikacije, Internet preglednici i uređaji
- Aktivnost
- Lokacija
- Lokalna pohrana, baze podataka, pikseli, kolačići i zapisnici poslužitelja

Aplikacije, Internet preglednici i uređaji prikupljaju podatke o broju verzije aplikacije, vrsti i postavkama preglednika, vrsti uređaja i postavkama istog, operacijskom sustavu terminalnog uređaja te podatke o mobilnoj mreži, operatoru i telefonskom broju.

Aktivnosti uključuju pojmove za pretraživanje na *Google-u*, videozapise koji su pogledani, interakcije i pregledi sadržaja i(li) oglasa, komunikaciju s ostalim korisnicima, povijest pregledavanja u *Chrome-u*, aktivnosti na web lokacijama i aplikacijama.

Google proizvodi imaju pristup GPS-u, IP adresi i podacima senzora za vrijeme korištenja aplikacija ili uređaja. Javne Wi-Fi pristupne točke i mobilni odašiljači obavještavaju *Google* o lokaciji korisnika.

Pikseli, kolačići, lokalna pohrana, baze podataka i zapisnici poslužitelja su tehnički detalji implementirani na web mjestu koje *Google* može pratiti, a povezani su s *Google* proizvodima i uslugama,[25].

Prema *Google* pravilima privatnosti pohrana i izvlačenje podataka izvodi se iz više izvora, ovisno o vrsti aplikacije ili usluge. Podatkovni profil stvara se osobnim i osjetljivim podacima kao što su ime i prezime, datum rođenja, adresa i lokacije. Uz osobne podatke podatkovni profil upotpunjuje se s podacima s uređaja, aplikacija i usluga.

Gmail podaci koje *Google* čita i pohranjuje su informacije iz svake e-pošte koju korisnik pošalje i primi te sve ostale mape, kao što su neželjena pošta, skice i obrisana e-pošta.

Google sprema svaku lokaciju mjesta koju korisnik posjećuje i traži na svojim uređajima neovisno o prijavljenom/neprijavljenom uređaju.

Google Hangouts sprema sve razgovore, a kalendar sprema i prikazuje podatke o tome gdje će se nalaziti korisnik i kad. *Google asistent* sprema svaki zahtjev odnosno pitanje koje se postavlja u glasovnom obliku koje se kasnije može preslušati.

Android uređaji rade na operativnom sustavu koji je izradio *Google*, a to omogućuje potpunu kontrolu i uvid u korištenje aplikacija, praćenje i personaliziranje oglasa. Vrijeme otvaranja i korištenja pojedine aplikacije se sprema te se sadržaj u tim aplikacijama prilagođava korisniku.

Podaci koje sprema i prikuplja u aplikacijama mogu se podijeliti na podatke koji se koriste za analitiku, podaci koji se koriste za personaliziranje proizvoda, za funkcionalnosti aplikacije te za oglašavanje i marketing.

Dijeljenje podataka potrebno je regulirati, a kako *Google* koristi i dijeli podatke s trećim stranama za relevantne i ciljane oglase te za personalizirani sadržaj, *Google* podatke može podijeliti isključivo iz sljedećih razloga:

1. Kad korisnik da privolu za dijeljene osobnih podataka
2. Ako *Google* zaprimi zahtjev od vlade za dijeljenje podataka iz pravnih razloga
3. Ako postoji administrator domene koji upravlja *Google* aplikacijama na poslu ili u obrazovanju
4. Kad *Google* treba tvrtku treće strane ili podružnicu za pomoć u obradi podataka,[25].

5. Ekstrakcija podataka Google usluga

Proces ekstrakcije podataka i dokaza s mobilnih telefona te forenzičko ispitivanje različitih mobilnih uređaja može se razlikovati ovisno o više čimbenika u procesu digitalne forenzike. Praćenje dosljednog procesa ispitivanja osigurati će istražitelju prikupljanje pouzdanih dokaza i dokumentiranje istih. Standardni proces za mobilnu forenziku ne postoji, ali se ovisno o vrsti uređaja i potrebi procesa forenzičke analize, odabire jedan od procesa izvlačenja dokaza ili metodologija. Prije odabira metodologije istražitelj se mora držati načela vezanih za lanac posjeda dokaza (eng. *Chain of custody*) te time osigurati integritet prikupljenih podataka te valjanost prikupljenih podataka kako bi takvi podaci bili prihvaćeni na sudu kao dokaz.

Sve metode ili metodologije koje se koriste pri izdvajanju (ekstrakciji) podataka s mobilnih uređaja trebaju biti testirane, potvrđene te detaljno i dobro dokumentirane. Ovisno o vrsti uređaja nad kojim se provodi forenzička analiza odabire se odgovarajuća metodologija digitalne forenzike mobilnih uređaja,[47].

5.1. Referentna metodologija forenzičke analize mobilnih uređaja

Referentna metodologija mobilne digitalne forenzike ili metodologija forenzičke analize izrađena je 2011. godine od strane SANS (eng. *Escal Instiute of Advanced Technologies*) instituta za obuku kibernetičke sigurnosti, certificiranje, diplome i resurse mobilnih uređaja te se sastoji se od 9 koraka:

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

1. Uvođenje

Uvođenje ili faza prikupljanja dokaza je početna faza koja uključuje papirologiju koja sadrži podatke o vlasništvu, vrsti incidenta u koji je mobilni uređaj bio uključen te vrstu podataka i informacija koje istražitelj prikuplja. Najvažniji dio ove faze je razvijanje specifičnih ciljeva za svako ispitivanje ili analizu. Prije nego što započne postupak fizičke zapljene uređaja i podataka potrebno je proučiti lokalne, savezne i državne zakone koji se odnose na prava pojedinca. Istražitelj mora poštovati ispravne procedure i pravila lanca posjeda dokaza, kako

bi podaci prikupljeni na taj načini bili zakoniti na sudu. Prilikom preuzimanja uređaja potrebno je podatke ostaviti u izvornom obliku i paziti da se ne promijene isti.

2. **Identifikacija**

Forenzički ispitivač mora identificirati pojedinosti za svako ispitivanje mobilnog uređaja, a to su zakonsko tijelo, podaci koji se trebaju ekstrahirati, pojedinosti mobilnog uređaja, mediji za pohranu podataka i drugi izvori potencijalnih dokaza. Tijekom faze identifikacije forenzički istražitelj mora razumjeti i poznavati zakonsku regulativu te poštovati pravila i norme koje su zatražene sudskim nalogom, tako da se poštuju načela lanca posjeda dokaza. Na temelju traženih podataka istražitelj utvrđuje koje je ispitivanje potrebno te koje je alate i tehnike potrebno odabrati. Ukoliko se mediji za pohranu podataka nalaze u mobilnom uređaju, uklanjaju se i obrađuju se digitalnim putem. Mobilni uređaj je potrebno identificirati prema:

- Nazivu proizvođača
- Modelu i boji uređaja
- Serijskom broju uređaja
- Prema vidljivoj pozadini na zaslonu uređaja
- Prema hardverskim komponentama
- Trenutnom stanju uređaja,[26],[27]

3. **Priprema**

Faza pripreme počinje nakon što je identificiran model mobilnog uređaja. Ova faza uključuje istraživanje pojedinosti uređaja te ispitivanje metoda i alata koji se koriste za akviziciju i analizu. Odabir alata i metoda ovisi o modelu, operativnom sustavu i verziji operativnog sustava uređaja. Na temelju toga odabire se potrebna hardverska i softverska oprema te kablovi za spajanje uređaja na forenzički alat.

4. **Izolacija**

Izolacija se izvodi prilikom akvizicije uređaja i za vrijeme procesa forenzičke analize. Izolacijom uređaja onemogućuje se i sprječava utjecaj, izmjena i brisanje podataka, odnosno dokaza s uređaja. Kad je telefon spojen na neku komunikacijsku mrežu mogu se dodati novi podaci putem poziva, poruka i podataka aplikacija, što mijenja dokaze na uređaju. Potpuno uništenje podataka moguće je i putem daljinskog pristupa ili naredbi za daljinsko brisanje.

Zaštita uređaja od komunikacijskih izvora kao što su mobilna mreža, Wi-Fi ili *Bluetooth* može se izvesti stavljanjem mobilnog uređaja u zrakoplovni način rada i postavljanje uređaja u radio frekventnu zaštitnu tkaninu. Alternativno rješenje je izolacija uređaja korištenjem Faradayeva kaveza ili vrećice koji blokiraju signal koji uređaj prima ili šalje. Kavez i vreća sadrže materijale koji blokiraju radiovalove i tako sprječavaju prolaz signala.

5. **Procesiranje**

Prvi korak u ovoj fazi je ekstrakcija podataka iz uređaja, a ukoliko postoji vanjski medij za pohranu podataka obrađuje se zasebno digitalnim putem. Najveći izazovi ove faze su identificiranje alata i odabir vrste ekstrakcije ovisno o cilju istrage. Kod ekstrakcije mobilnih uređaja često će biti potrebno koristiti više alata kako bi se izvela željena ekstrakcija podataka i dokaza. Fizička ekstrakcija je najčešća metoda ekstrakcije zato što se ekstrahiraju neobrađeni podaci iz memorije te se uređaj isključuje tijekom procesa ekstrakcije. Ako ova metoda ne uspije, odrađuje se datotečna ekstrakcija. Logička ekstrakcija se uvijek izvodi zato što može sadržavati raščlanjene podatke,[26].

6. **Verifikacija**

Prvi korak nakon procesiranja mobilnog uređaja je provjera točnosti podataka dobivenih ekstrakcijom mobilnog uređaja. Provjera ekstrahiranih podataka može se postići na nekoliko načina, a jedan od načina je provjera ekstrahiranih podataka s trenutnim podacima na uređaju. Ekstrahirani podaci se uspoređuju s podacima logičke ekstrakcije ili s podacima na samom uređaju. Drugi način je korištenje više alata za forenzičku analizu i uspoređivanje dobivenih rezultata. Treći način je upotreba *hash* vrijednosti koja predstavlja jedinstveni ID datoteke i podataka u mobilnom uređaju.

7. **Dokumentiranje**

Istražitelj je dužan tijekom cijelog postupka ispitivanja mobilnog uređaja dokumentirati sve korake i sve što je učinjeno za vrijeme akvizicije uređaja i podataka. Nakon završetka istrage dokumentirani podaci trebaju proći stručni pregled kako bi se osiguralo da su podaci točni i provjereni te da je istraga dovršena. Dokumentacija mora sadržavati informacije kao što su:

- Datum i vrijeme početka forenzičkog ispitivanja
- Fizičko stanje uređaja
- Fotografije uređaja i pojedinačnih komponenti
- Status uređaja kada je primljen (uključen/isključen)
- Model uređaja
- Alati korišteni u ekstrakciji i analizi
- Pronađeni podaci

8. **Prezentacija**

Tijekom istrage je važno osigurati da se informacije koje su ekstrahirane i dokumentirane s mobilnog uređaja mogu jasno prezentirati na način da su razumljive drugim istražiteljima na

sudu ili trećim stranama. Forenzičko izvješće uključuje podatke u papirnatom i digitalnom obliku. Prezentirani dokazi moraju dokumentirani na način da su jasni, sažeti i repetitivni.

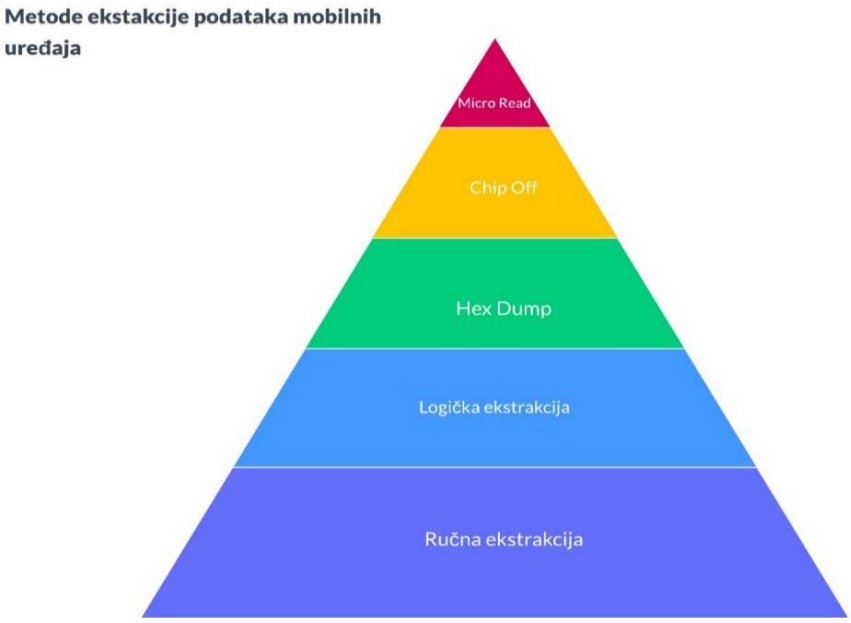
9. Arhiviranje

Arhiviranje i čuvanje podataka dobivenih ekstrakcijom je važan dio cjelokupnog procesa forenzičke analize. Podaci se trebaju čuvati u upotrebljivom formatu za sudski proces koji je u tijeku, za buduću upotrebu, za vođenje evidencije te, ako se trenutni dokazi unište ili oštete. Zbog dugog vremenskog trajanja sudskih procesa, dokazi moraju biti arhivirani i dostupni u svako vrijeme[26],[27].

5.2. Forenzičke procedure i metode ekstrakcije podataka

Potrebna razina ekstrakcije i analize ovisi o zahtjevu i specifičnostima istrage i vrste uređaja. Ovisno o parametrima uređaja i istrage te procedurama, određuje se metoda ekstrakcije i analize. Više razine ekstrakcije zahtijevaju dodatne vještine ispitivača i opsežnije ispitivanje, koje možda neće biti primjenjive za svaki uređaj ili situaciju. Jedina standardna procedura koju je potrebno slijediti je stavljanje mobilnog uređaja u način rada u zrakoplovu (engl. *Airplane mode)* kako bi se onemogućio udaljeni pristup uređaju. Procedure i metode ekstrakcije podataka mogu se opisati i prikazati pomoću mobilne forenzičke piramide za klasifikaciju alata i metoda. Na slici 10. prikazane su metode ekstrakcije podataka mobilnih uređaja te invazivne metode fizičke ekstrakcije. Metode ekstrakcije podataka dijele se na:

1. Ručna ekstrakcija
2. Logička ekstrakcija
3. Datotečna ekstrakcija
4. Fizička ekstrakcija (*Hex Dump / JTAG, Chip-off, Micro Read*)



***Slika 10**. Metode ekstrakcije podataka mobilnih uređaja, [28]*

Cilj sustava klasifikacije metoda ekstrakcije podataka mobilnih uređaja je omogućiti forenzičaru kategorizaciju alata na temelju metodologije ispitivanja alata. Od dna prema vrhu piramide, metode i alati koji se koriste postaju sofisticiraniji i potrebno je više vremena kako bi se odradila analiza. Svaki od ovih sustava ili slojeva ima svoje prednosti i mane s kojima je upoznat forenzički ispitivač te na temelju svih podataka i zahtjeva odabire potrebnu metodu. Kao najbitnija stavka za odabir metode ističe se obuka forenzičkog ispitivača. Dokazi mogu biti potpuno uništeni, ako se koristi neodgovarajuća metoda ili alat,[28].

1. **Ručna ekstrakcija**

Metoda ručne ekstrakcije je najjednostavnija metoda ekstrakcije podataka mobilnih uređaja koja uključuje jednostavno pregledavanje i pomicanje podataka na uređaju pomoću mehaničkog pomagala (tipkovnice) ili zaslona osjetljivog na dodir. Informacije i podaci se spremaju na način da se fotografiraju nekim drugim mobilnim uređajem ili fotoaparatom. Proces ekstrakcije je brz i jednostavan za korištenje te se može primijeniti na gotovo svakom mobilnom uređaju. Jedini preduvjet za ekstrakciju je otključan uređaj ili poznavanje lozinke uređaja. Ručna ekstrakcija podliježe i sklona je ljudskim pogreškama, a postoji i problem nedostatka određenih podataka zbog nepoznavanja sučelja uređaja. Druga mana ovog pristupa i metode je nemogućnost oporavka izbrisanih podataka i ekstrakcija svih podataka, pa se ne može očuvati integritet podataka i samog uređaja. Postoje alati koji mogu olakšati proces ekstrakcije (*Project-A-Phone*) svih podataka, ali nije moguće pristupiti izbrisanim podacima[26],[29].

2. **Logička ekstrakcija**

Logička analiza uključuje povezivanje mobilnog uređaja s forenzičkom hardverskom komponentnom ili radnom stanicom putem USB kabela, RJ-45 kabela, *Bluetootha* ili infracrvenog povezivanja. Povezano računalo pokreće naredbu i šalje je prema uređaju koju interpretira procesor uređaja. Traženi podaci primaju se iz memorije uređaja i prosljeđuju na forenzičku radnu stanicu. Većina forenzičkih alata podržava logičku ekstrakciju, a metoda zahtjeva kratkotrajnu obuku te sama ekstrakcija ne traje dugo. Logička ekstrakcija omogućuje ekstrakciju veće količine podataka i informacija u usporedbi s ručnom ekstrakcijom. Nedostatak metode je izmjena ili zanemarivanje određenih podataka, kao što su nepročitani SMS te ne prikuplja podatke koji su izbrisani, a time se narušava integritet dokaza.

Uređaji zaštićeni lozinkom ili zaključani uređaji ne mogu se ekstrahirati ovom metodom. Logička ekstrakcija može se podijeliti na Agentski temeljenju ekstrakciju i ekstrakciju korištenjem ADB (*Android Debug Bridge*)[26],[30].

3. Datotečna ekstrakcija

Datotečna ekstrakcija ili *File system* ekstrakcija je proširenje logičke ekstrakcije koja omogućuje forenzičkom ispitivaču analizu datotečnog sustava u cjelini, a ne samo pojedine dijelove sustava. Može uključivati obrisane ili skrivene podatke, ako se odabere odgovarajuća metoda pohrane podataka te log datoteke unutar tog sustava. Ovakva metoda je detaljnija od logičke, a omogućuje ekstrakciju detaljnijih informacija iz aplikacija, kao što su web povijest, podaci o e-pošti i medijima te povijest odredišta *Google* karata. Datotečna ekstrakcija zahtijeva dekodiranje podataka datotečnog sustava i baza podataka zato što su ekstrahirani podaci neobrađeni. Klasične metode datotečne ekstrakcije su:

- *Android Debug Bridge*
- *Android Backup*
- *Android Backup APK downgrade*

Metoda datotečne ekstrakcije koju je moguće provesti *s UFED Touch 2* ili *UFED 4PC* alatima je selektivna datotečna ekstrakcija, a omogućuje odabir onih podataka koji se mogu legalno prikupiti s *Android* uređaja,[31], [32].

4. Fizička ekstrakcija

Fizička ekstrakcija mobilnog uređaja je kopiranje podataka koji se nalaze na fizičkom mediju, na kojem se vrši analiza metodom *bit-by-bit.* Opisuje se kao najopsežnija i najzahtjevnija metoda ekstrakcije s najmanjom podrškom. Ovom metodom se ispitivaču osigurava potpuna kopija memorije uređaja, kako bi se mogli ti podaci točno interpretirati. UFED koristi *Bootloader* kako bi se prekinuo standardni postupak podizanja operativnog sustava i omogućio da se uređaj koristi u načinu rada za čitanje, čime bi se sačuvao integritet dokaza i podaci bi bili nepromijenjeni.

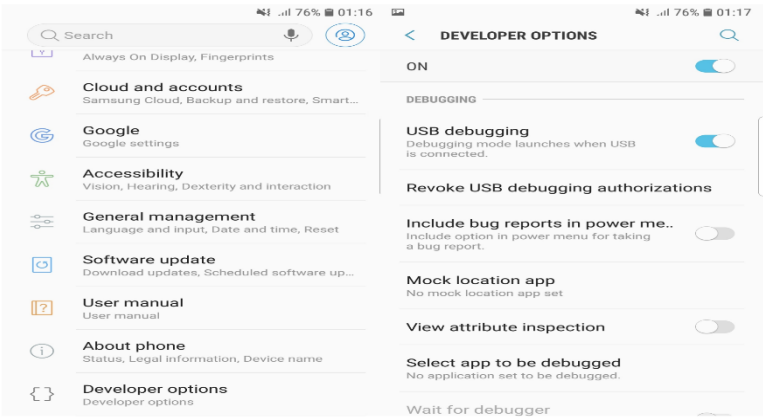
Fizičkom ekstrakcijom se prikupljaju informacije o vremenskim podacima aplikacija, sistemskim datotekama i izbrisanim datotekama uz sve podatke koji se prikupljaju logičkom ekstrakcijom. Metoda omogućuje pristup bazama podataka, a samim time i GPS lokacijama, Bluetooth vezama i bežičnim mrežama. Može se podijeliti na neinvazivne i invazivne fizičke ekstrakcije. *Clinet*, *Android Debug Bridge, Bootloader i Forensic Recovery Partition* su neinvazivne metode ne zahtijevaju fizičko rastavljanje uređaja. Invazivne metode koje zahtijevaju fizičko rastavljanje uređaja jesu *JTAG, Chip off,* i *Micro Read*, [32],[33].

5.3. Postupak ekstrakcije Google podataka s mobilnog uređaja

Postupak ekstrakcije podataka započinje pripremom mobilnog uređaja *Samsung Galaxy S7 Edge* na kojem će se provoditi ekstrakcija te pripremom forenzičkog alata *UFED Touch 2* s kojim će se provoditi odgovarajuća metoda ekstrakcije podataka. Dobiveni podaci i

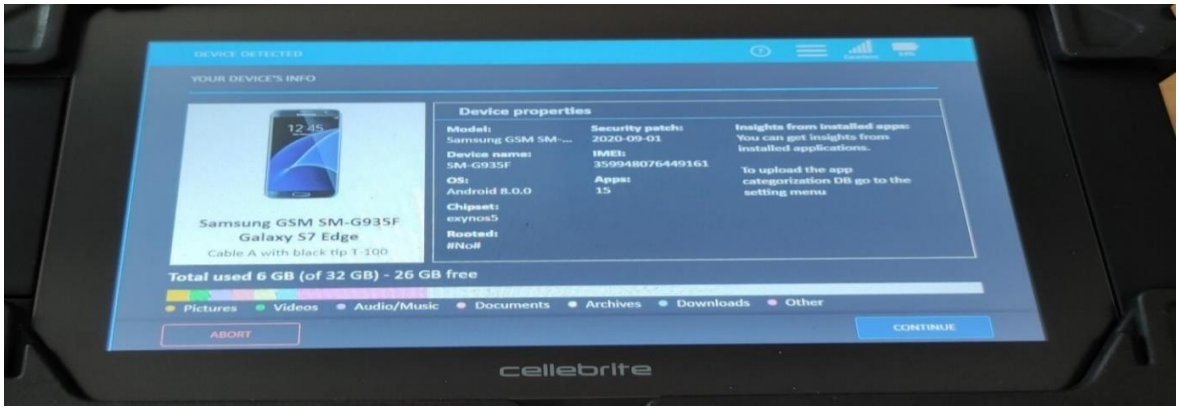
informacije će se pohraniti na vanjskom tvrdom disku. Detaljan opis pripreme uređaja i alata su objašnjeni u prethodnim poglavljima. Praktični dio ovog diplomskog rada, postupak ekstrakcije i forenzičke analize izvršen je u Laboratoriju za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava.

Prije početka ekstrakcije uređaja potrebno je omogućiti *Android debug bridge* (ADB) alat koji omogućuje komunikaciju s *Android* uređajem i kontrolu nad njim. Potrebno je uključiti sakriveni alat u postavkama koji se naziva *Developer Options* ili opcije za razvojne programere. Alat je sakriven kako bi se spriječilo slučajno omogućavanje alata, a pristup alatu moguć je kombinacijom 7 dodira zaslona u postavkama uređaja. Dodatna sigurnosna opcija je sigurno USB otklanjanje pogrešaka, a te postavke su prikazane na slici 11, [34].



***Slika 11**. Android Debugging bridge i Developer options*

Nakon što su zadovoljeni svi uvjeti pripreme *UFED Touch 2* alata, terminalni uređaj na kojem se provodi ekstrakcija stavlja se u izolaciju postavljanjem uređaja u zrakoplovni način. Time se sprječava moguće brisanje ili mijenjanje podataka, čime bih se narušio lanac posjeda dokaza i integritet dokaza. Nakon što se povežu mobilni uređaj i vanjski tvrdi disk s hardverskom komponentom forenzičkog alata, na zaslonu *UFED Touch 2* alata odabire se komponenta nad kojom će se vršiti ekstrakcija te je to u ovom slučaju mobilni uređaj. Forenzički alat nudi mogućnost automatskog prepoznavanja mobilnog uređaja nakon što se uređaj spoji kablom, kao što je prikazano na slici 12.



***Slika 12**. Automatsko prepoznavanje mobilnog uređaja, UFED Touch 2*

Sljedeća faza je odabir željene metode ekstrakcije. U diplomskom radu vršiti će se tri različite metode. Postupak ekstrakcije podataka za fizičku, logičku i datotečnu ekstrakciju je vrlo sličan te nije potrebno opisivati postupak ekstrakcije za svaku metodu posebno. Nakon odabira jedne od ekstrakcija, potrebno je odabrati mjesto pohrane ekstrahiranih podataka. Mjesto pohrane podataka za sve ekstrakcije je vanjski tvrdi disk koji je povezan s mobilnim uređajem i radnom stanicom forenzičkog alata. *UFED Touch 2* alat nudi mogućnost odabira vrste podataka i datoteka koje se ekstrahiraju, pa se na taj način može usredotočiti na *Google* podatke i aplikacije. Odabirom željenih podataka i datoteka započinje ekstrakcija podataka i ovisno o metodi, potreban je određeni vremenski period za obavljanje iste. Nakon što je ekstrakcija uspješno obavljena, dobiva se sažetak ekstrakcije sa svim vrstama podataka koje su pronađene na uređaju. Završni dio ekstrakcije je generiranje i pohrana izvješća. Na slici 13. prikazano je radno okruženje potrebno za ekstrakciju podataka pomoću *UFED Touch 2.*

***Slika 13**. Ekstrakcija podataka s mobilnog uređaja*

Podaci dobiveni ekstrakcijom uređaja mogu se podijeliti u više grupa. Najosnovnija podjela je na kategorizirane i nekategorizirane podatkovne datoteke. U kategorizirane podatkovne datoteke pripadaju: Aplikacije, arhivi, zvučne datoteke, baze podataka, dokumenti, slike i tekst, a u drugu skupinu pripadaju sve ostale datoteke koje se iz nekog razloga ne mogu grupirati. Metode ekstrakcija koje se analiziraju u diplomskom radu su:

- Logička ekstrakcija (Vrijeme trajanja ekstrakcije- 35 minuta)
- Datotečna ekstrakcija (Vrijeme trajanja ekstrakcije- 48 minuta)
- Fizička ekstrakcija (Vrijeme trajanja ekstrakcije- 41 minuta)

6. Analiza prikupljenih podataka Google usluga

Praktični dio diplomskog rada podijeljen je u dvije grupe. Prvi dio ili prva grupa je ekstrakcija Google podataka korištenjem *UFED Touch 2* alata. Drugi dio praktičnog rada je generiranje izvještaja i analiza podataka korištenjem forenzičkog alata *Cellebrite Reader*. Forenzički alat omogućuje uvid u sve podatke koje je korisnik generirao te podatke koje su spremale određene aplikacije ili web stranice. Podaci o uređaju nad kojim se provodila forenzička analiza prikazani su na slici 14.

Device Info

Advertising Id	0e3cae7d-b2a2-4b24-9b14-ca65fd72f0ab
Android fingerprint	samsung/hero2ltexx/hero2lte:8.0.0/R16NW/G935FXXU8ETI2:u...
Bluetooth MAC Address	8C:1A:BF:B5:C2:75
Android ID	bd04e3fc3a6b8e87
Bluetooth device address	8C:1A:BF:B5:C2:75
Bluetooth device name	Galaxy S7 edge
Carrier Name	No network connection
Current SIM Country ISO	hr
Current SIM Operator	21910
Current SIM Operator Name	A1 HR
Detected Phone Model	SM-G935F
Detected Phone Vendor	samsung
Factory number	RF8H52BRRCJ
Location Services Enabled	True
Mock locations allowed	False
OS Version	8.0.0
SIM Change Operation	3
Time Zone	(UTC+01:00) Zagreb (Europe)
ICCID	8938591420081233957
IMSI	219101137239185
Mac Address	4C:66:41:40:F9:1B
Phone Activation Time	5/10/2021 6:25:15 PM(UTC+0)
Recovery Event	2019-02-17T13:32:24.000+01:00

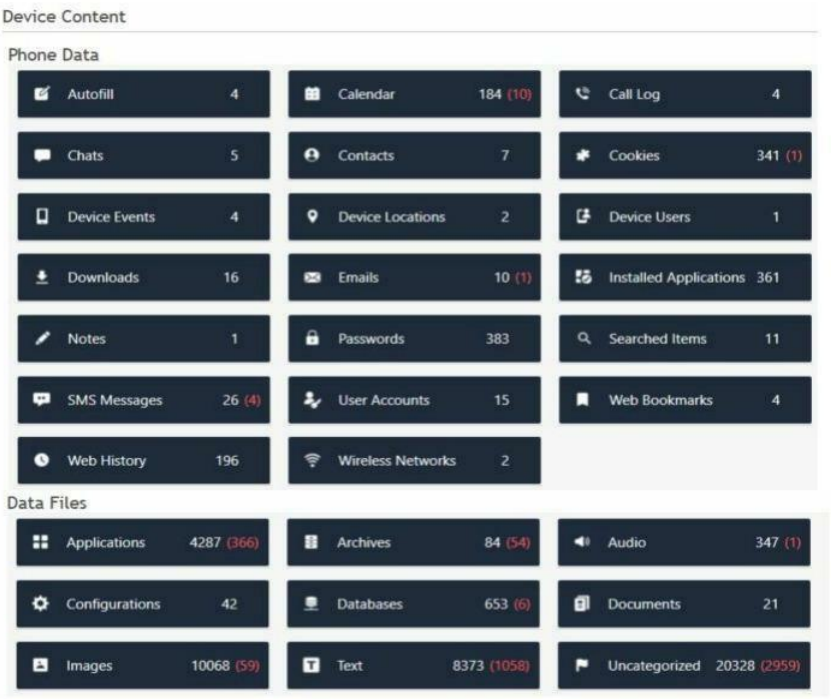
***Slika 14**. Podaci o uređaju generirani u Cellebrite Reader alatu*

Osim osnovnih podataka uređaja prikazana je aktivacija uređaja te zadnji pokušaj oporavka podataka. Uz osnovne podatke uređaja pohranjuju se informacije o bežičnim mrežama na kojima je spojen uređaj, odnosno s kojima komunicira. Svaki *Android* uređaj ima jedinstven ID oglašavanja (*Advertising ID*) koji omogućuje korisnicima bolju kontrolu, a programerima pruža jednostavan i standardan sustav za rad. ID oglašavanja pružaju *Google Play* usluge čiji su cilj personalizirane reklame. Pred kraj 2021. godine *Google Play* usluge omogućile su korisnicima uklanjanje ID-ja prilikom određivanja personalizirane kontrole, [35].

Ekstrahirani podaci koji se analiziraju skupno se nazivaju sadržaj uređaja te se mogu podijeliti u dvije skupine. Prva skupina su podaci uređaja koji sadrže podatke o razgovorima, kontaktima, lokacijama uređaja, preuzimanjima na uređajima, lozinkama, i sličnim podacima. Druga skupina su datoteke s podacima kao što su aplikacije, arhivi, baze podataka, slike, audio datoteke i dokumenti. Na slici 15. prikazane su grupe podataka fizičke ekstrakcije.

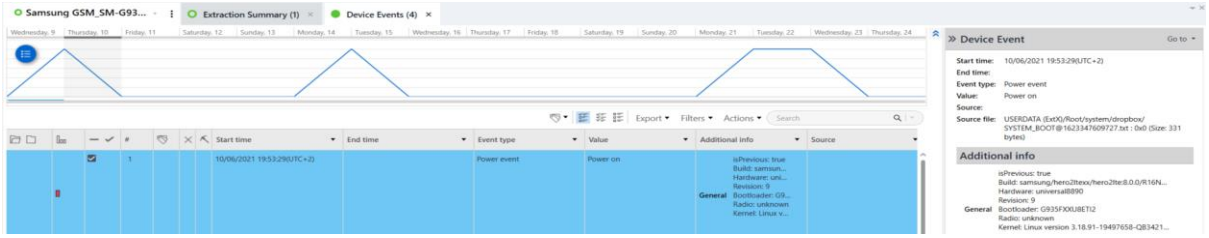
Analiziranje podataka u forenzičkom alatu *Cellebrite Reader* može se obaviti grupiranjem podataka koje omogućuje analizu pojedinih vrsta podataka, datoteka ili baza podataka, te

korištenjem vremenske crte (Eng. *Timeline*) koja prikazuje podatke prema vremenskom redoslijedu. Vremenska crta prikazuje vremenski ovisne podatke za koje je poznato vrijeme generiranja, kreiranja ili ako se radi o slikama vrijeme fotografiranja. Na vremenskoj crti prikazuju se slike, kalendar, e-pošta, povijest Internet pretraživača, SMS poruke, pozivi, instalirane aplikacije, web kolačići, bilješke, preuzimanja te pojmovi pretraživanja u Internet pretraživačima.



Slika 15. *Grupiranje podataka nakon ekstrakcije.*

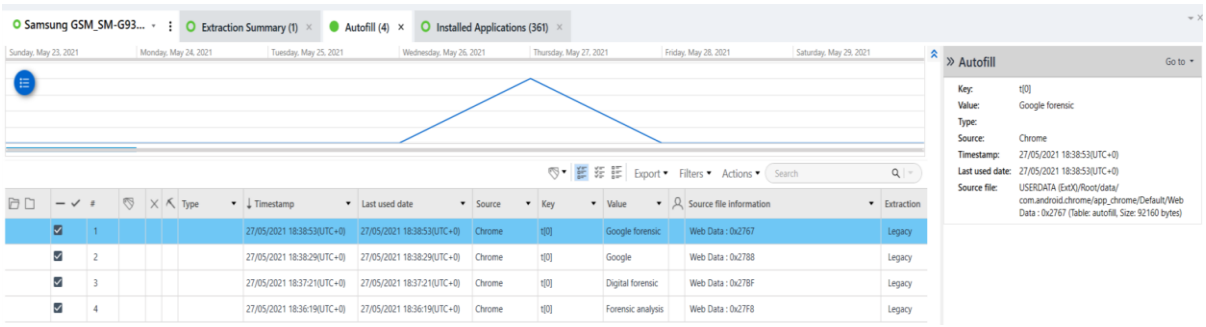
Grupiranje podataka slično je u fizičkoj i datotečnoj ekstrakciji, dok se logičkom ekstrakcijom ne prikazuju lokacije uređaja, korisnici uređaja, lozinke, bežične mreže te događaji odvojeni od operacijskog sustava uređaja. Takvi događaji se pohranjuju, kao pokretanje uređaja odnosno mehaničko paljenje uređaja, a u ovom slučaju mobilnog uređaja na tipku ili kombinaciju tipki. Ekstrakcijom uređaja i analizom podataka zabilježena su četiri događaja pod nazivom *Power event*, prikazana su na slici 16.



Slika 16*. Prikaz događaja uređaja u Cellebrite Reader alatu*

6.1 Prikupljanje i analiza podataka uređaja

Google prikuplja podatke iz različitih aplikacija i usluga, koje se pohranjuju u terminalnom uređaju te na *Cloud* serverima. Ekstrahirani podaci spremaju se i zapisuju u različite baze podataka, a kao skup podataka nazivaju se *Userdata* ili u slobodnom prijevodu korisnički podaci. Pohranjeni mogu se pregledati korištenjem *Cellebrite Reader* alata. *Google Chrome* aplikacija i Internet pretraživač omogućuju automatsko popunjavanje ili predviđanje teksta koji korisnik upisuje u tražilicu. *Google Chrome* pretraživač pohranjuje ključne riječi u pripadajuće datoteke i baze podataka.



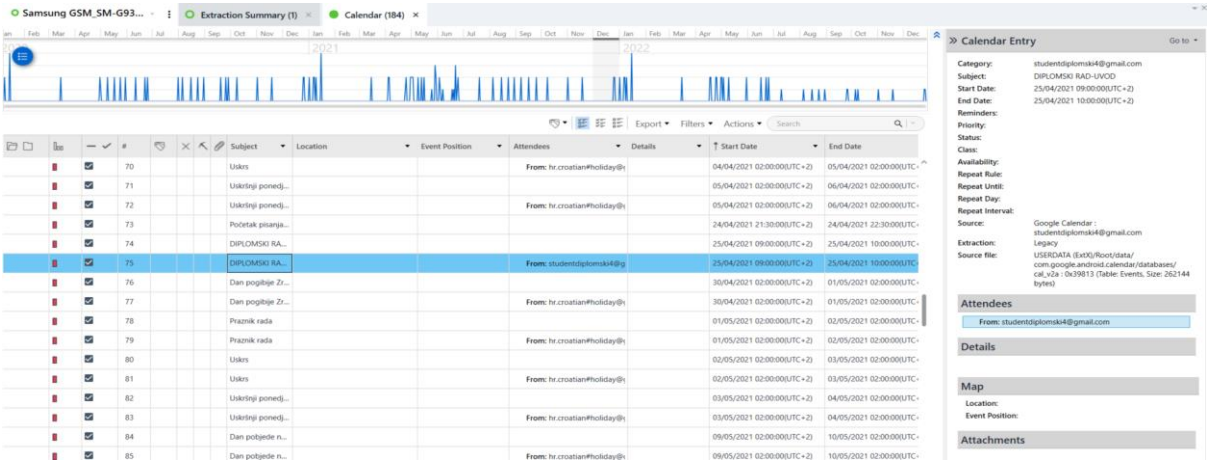
Slika 17. *Automatsko popunjavanje ključnih riječi.*

Vremenska oznaka ključne riječi pohranjena je te pokazuje kad je prvi put korištena napredna naredba automatskog popunjavanja upisanog teksta. Također su pohranjeni datum zadnjeg korištenja, izvor te vrijednost podataka (ključne riječi) prikazani na slici 17. *Google Chrome* Internet pretraživač pohranjuje podatke kao što su povijest pregledavanja Internet stranica, koji su izravno povezani sa pretraženim pojmovima, korisničke profile, lozinke te web kolačiće.

Slika 18. *Usporedba pohranjenih kolačića na domeni google.com*

Na slici 18. prikazana je usporedba kolačića u *Google Chrome* i *Android browser* pretraživaču. Kolačići prikupljaju podatke o korisniku, način na koji se korisnik ponaša online, lokaciju, specifikacije uređaja, pretraživanja u pregledniku, broj klikova na zaslonu uređaja, kako bi se identificirao pojedini korisnik i poboljšalo korisničko iskustvo na internetu,[36].

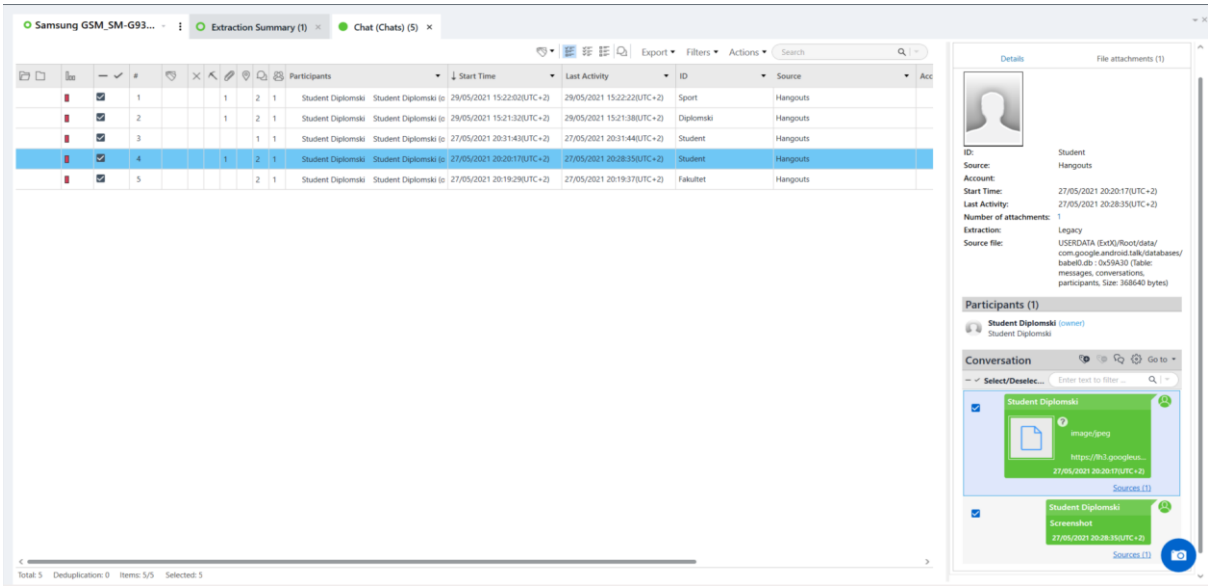
Ekstrakcijom podataka *Google* kalendar aplikacije dohvaćena su dva različita izvora podataka. Korisnički dio podataka su ručno uneseni događaji na mobilnom uređaju. Korištenjem uređaja te prilagođavanjem vremenske zone i geografskog područja (odabir regije), automatski se ažuriraju praznici i blagdani za odabranu regiju. Uz navedene podatke ekstrahirani su obrisani događaji pod nazivom dnevni plan.



***Slika 19**. Podaci u aplikaciji Google kalendar*

Na slici 18. prikazani su svi tipovi podataka koje aplikacija može prikupljati ovisno o željenim preferencijama. Osnovni podaci koji se prikupljaju su vrijeme, datum, izvor podataka, kategorija i naziv događaja.

Čavrljanje ili razgovori koji su se odvijali preko aplikacije *Google Hangouts* odvojeni su od klasičnih SMS poruka, te se prilikom ekstrakcije grupiraju u različite kategorije ekstrahiranih podataka. Ekstrahirani podaci su vrijeme početka razgovora, vrijeme zadnje aktivnosti, broj priloženih datoteka, te sudionici razgovora. Na slici 19. prikazan je produkt ekstrakcije za aplikaciju *Google Hangouts*.



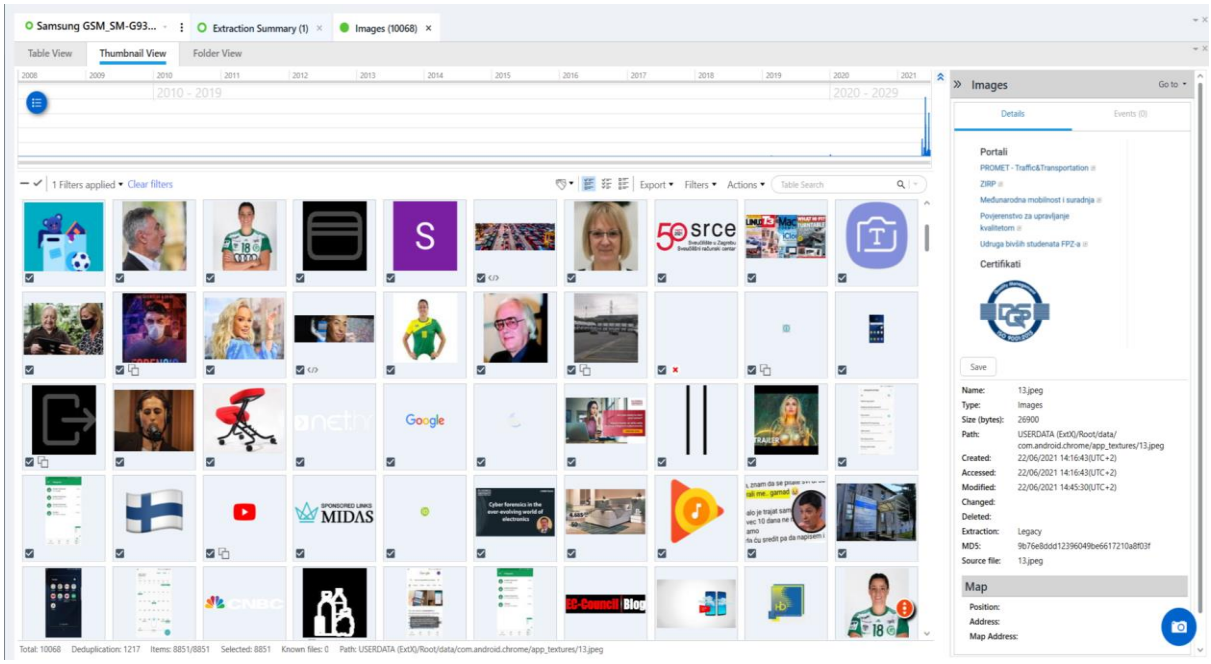
***Slika 20.** Google Hangouts aplikacija*

Source file ili izvorišna datoteka u svom izvornom obliku prikazuje bazu podataka u kojoj se pohranjuju svi podaci aplikacije te memorijski prostor koji zauzima pojedini razgovor. Naziv baze podataka u kojoj su pohranjeni podaci je *babel0.db*, a veličina memorijskog prostora koji zauzima svaki od 5 razgovora je 368640 bajta ili 0.3515 Megabajta.

6.2 Analiza podatkovnih datoteka u mobilnom uređaju

Podatkovna datoteka je svaka datoteka koja sadrži informacije, bez programskog koda. Takve datoteke su namijenjene za pregledavanje i čitanje, a pošto ne sadrže kod nisu namijenjene za izvršavanje. Programi se oslanjaju na podatkovne datoteke za dobivanje informacija. Podatkovna datoteka može sadržavati postavke programa koje programu daju smjernice na koji način se treba prikazati pojedina informacija. Mogu se instalirati zajedno s aplikacijom ili ih mogu kreirati korisnici. Većina takvih datoteka se pohranjuje u binarnom formatu, iako postoje datoteke koje pohranjuju podatke kao običan tekst,[37].

Prije nego što je obavljena fizička ekstrakcija terminalnog uređaja, na uređaju je generirano 25 slika iz različitih izvora. Nakon što je obavljena ekstrakcija uređaja, analizom podataka pronađeno je 10068 slika, od kojih je 59 slika obrisano.



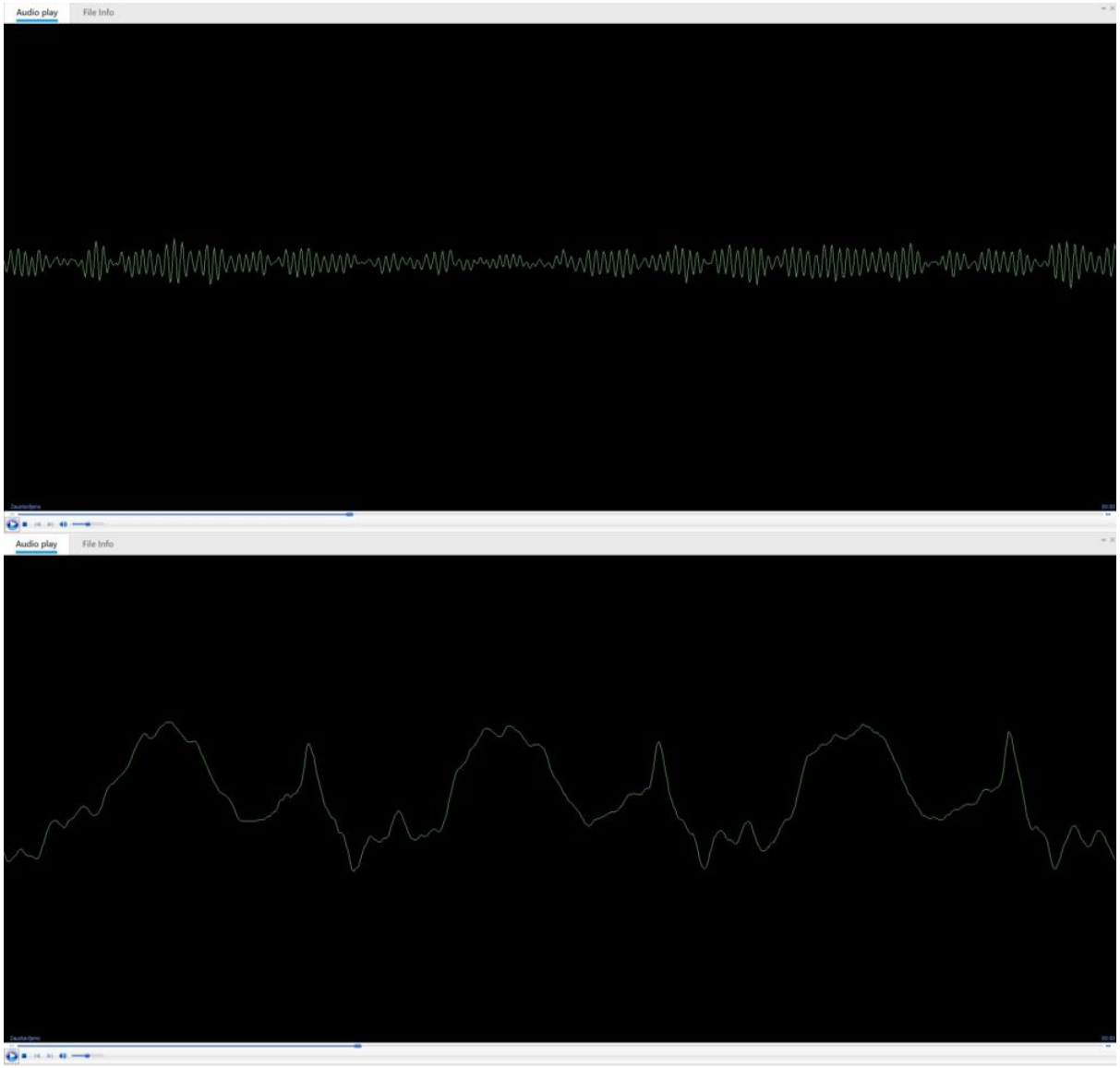
Slika 21. *Slike pohranjene u memoriji terminalnog uređaja*

Na slici 21. prikazan je dio slika pohranjenih na uređaju. Razlog velikog broja ekstrahiranih slika je način na koji *Google* aplikacije i usluge pohranjuju podatke. *Google Chrome* preglednik pohranjuje slike koje se pregledavaju, slike oglasa, slike na različitim internet stranicama, slike novinskih članaka. Sve takve slike se pohranjuju u priručnoj memoriji (eng. *Cache* memorija) uređaja.

Ekstenzija datoteke ili format datoteke ovisno o vrsti slike može biti *.jpeg (*engl. *Joint Photographic Experts Group), .png (*engl. *Portable Network Graphics), .jpg. te .webp(Web*

Picture Format). Osim slika pohranjene su sličice ili fotografije koje je moguće odabrati u *Google* tipkovnici, te *Samsung* „Emoji“ sličice u boji.

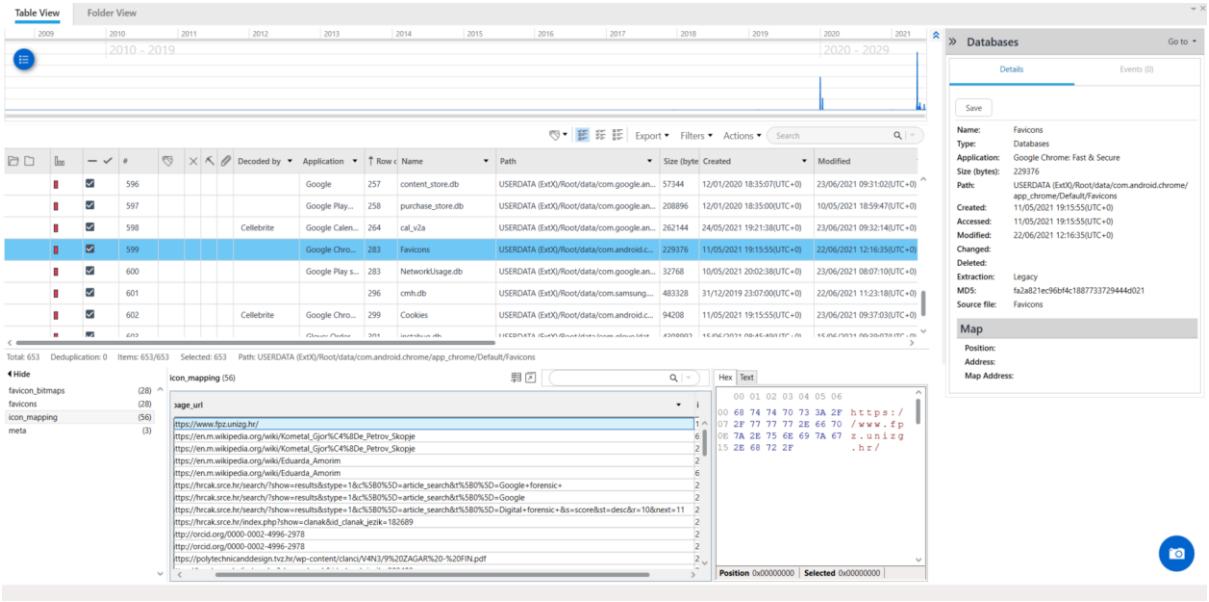
Audio ili zvučni zapisi pronađeni na uređaju su zvučne naredbe i zvučna signalizacija sistemskih aplikacija, audio zapisi aplikacije *Google* Karte te unaprijed ugrađeni i pohranjeni zvukovi. Audio zapisi sistemskih aplikacija su različiti zvukovi za obavijesti, poruke, pozive, alarme te odbrojavanja. Dodatni ekstrahirani sistemski audio zapisi su zvukovi otključavanja i zaključavanja uređaja, zvuk pokretanja operativnog sustava i isključivanje uređaja te upozorenja za praznu bateriju uređaja i zagrijavanje baterije. Takvi zvučni zapisi imaju .ogg (*Open-source file format for multimedia*) format datoteke koji je potrebno pretvoriti u Mp3 (engl. *Moving Picture Experts Group Layer-3 Audio*) format kako bi se preslušao sadržaj takve datoteke.



Slika 22. *Prikaz zvučnog zapisa u Cellebrite Reader alatu*

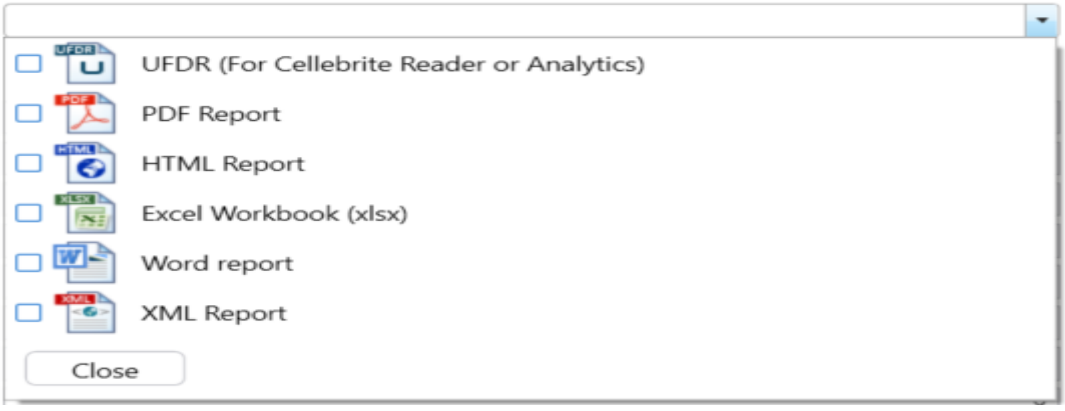
Na slici 22. prikazano je reproduciranje zvučnog zapisa „Izgubljen GPS signal“ ekstrahiranog iz aplikacije *Google* Karte na mobilnom uređaju, a u aplikaciji je pronađeno ukupno 165 zvučnih zapisa ili signalizacija. Naziv izvorišne datoteke prikazane na slici je *„._GPS_LOST.mp3*“.

Na mobilnom uređaju fizičkom ekstrakcijom pronađene su 653 baze podataka. Za svaku bazu podataka poznat je naziv, vrsta, naziv aplikacije za koju se generira baza podataka, veličina, vrijeme kreiranja i pristupa, izvorišna datoteka. Pretraživanje stranica u *Google Chrome* aplikaciji, posjećene stranice i podaci o stranicama pohranjuju se u zasebne baze podataka.



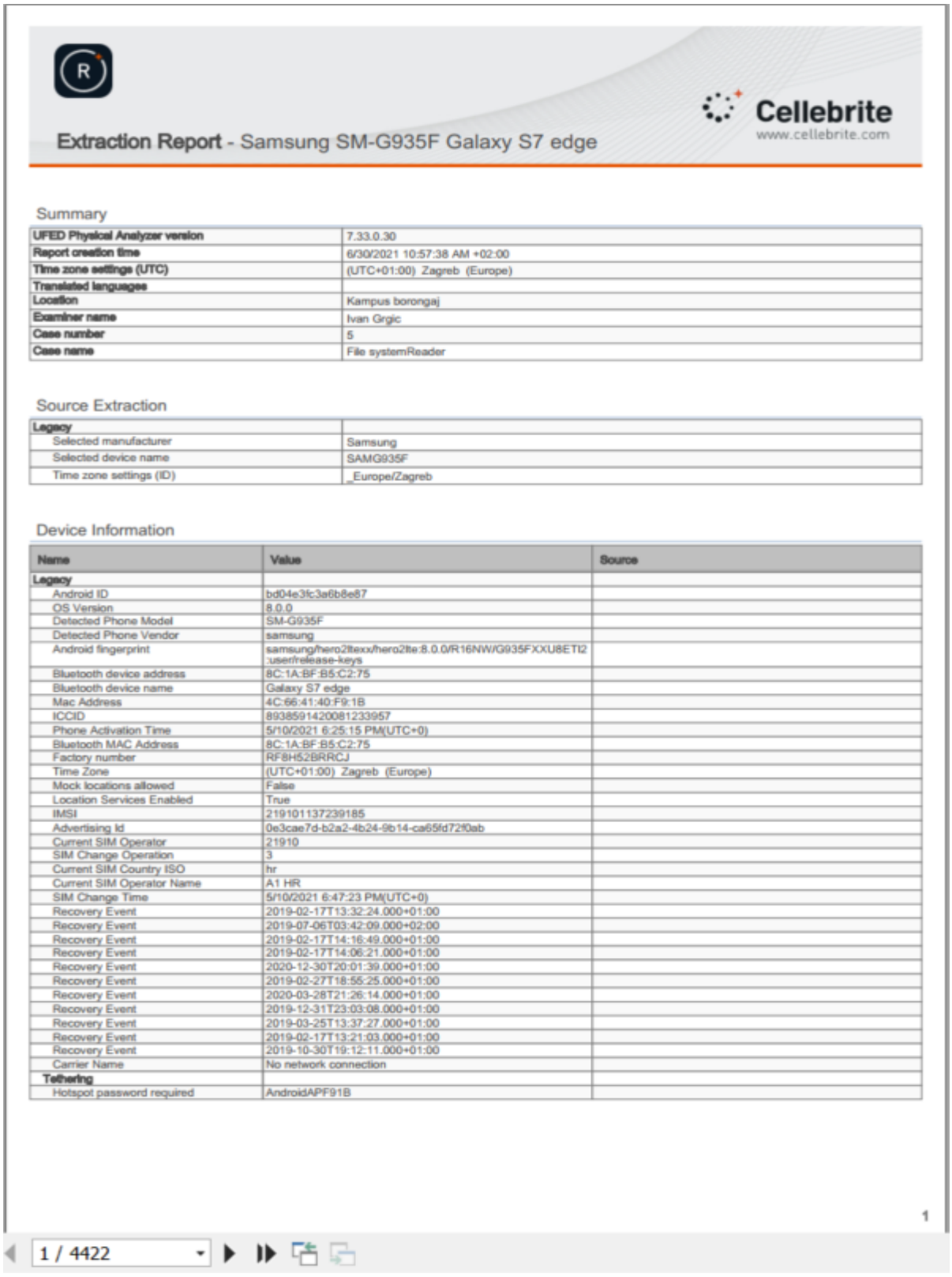
Slika 23. *Prikaz baze podataka i heksadekadski zapis web stranice*

Na slici 23. prikazana je baza podataka povezana sa *Google Chrome* aplikacijom te tekstualni zapis web stranice https://www.fpz.unizg.hr/ i heksadekadski zapis podijeljen u četiri različita niza. Format datoteke je *Favicons* što je skraćeni naziv za *Favourite icon* (omiljena ikona). To je datoteka koja sadrži jednu ili više ikonica, koje su povezane s određenom web stranicom,[37]. Na slici 24. prikazani su Formati u kojima je moguće generirati izvještaj ekstrahiranih podataka. Generiranjem izvještaja u željenom formatu omogućuje se lakše pretraživanje i filtriranje podataka, te jednostavnije snalaženje i analiziranje podataka.



Slika 24*. Generiranje izvještaja u UFED Reader alatu*

Na slici 25. prikazana je prva stranica izvještaja fizičke ekstrakcije u PDF formatu. Generirani izvještaj ima 4422 stranice.



Extraction Report - Samsung SM-G935F Galaxy S7 edge

Cellebrite
www.cellebrite.com

Summary

UFED Physical Analyzer version	7.33.0.30
Report creation time	6/30/2021 10:57:38 AM +02:00
Time zone settings (UTC)	(UTC+01:00) Zagreb (Europe)
Translated languages	
Location	Kampus borongaj
Examiner name	Ivan Grgic
Case number	5
Case name	File systemReader

Source Extraction

Legacy	
Selected manufacturer	Samsung
Selected device name	SAMG935F
Time zone settings (ID)	_Europe/Zagreb

Device Information

Name	Value	Source
Legacy		
Android ID	bd04e3fc3a6b8e87	
OS Version	8.0.0	
Detected Phone Model	SM-G935F	
Detected Phone Vendor	samsung	
Android fingerprint	samsung/hero2ltexx/hero2lte:8.0.0/R16NW/G935FXXU8ETI2 :user/release-keys	
Bluetooth device address	8C:1A:BF:B5:C2:75	
Bluetooth device name	Galaxy S7 edge	
Mac Address	4C:66:41:40:F9:1B	
ICCID	8938591420081233957	
Phone Activation Time	5/10/2021 6:25:15 PM(UTC+0)	
Bluetooth MAC Address	8C:1A:BF:B5:C2:75	
Factory number	RF8H52BRRCJ	
Time Zone	(UTC+01:00) Zagreb (Europe)	
Mock locations allowed	False	
Location Services Enabled	True	
IMSI	219101137239185	
Advertising Id	0e3cae7d-b2a2-4b24-9b14-ca65fd72f0ab	
Current SIM Operator	21910	
SIM Change Operation	3	
Current SIM Country ISO	hr	
Current SIM Operator Name	A1 HR	
SIM Change Time	5/10/2021 6:47:23 PM(UTC+0)	
Recovery Event	2019-02-17T13:32:24.000+01:00	
Recovery Event	2019-07-06T03:42:09.000+02:00	
Recovery Event	2019-02-17T14:16:49.000+01:00	
Recovery Event	2019-02-17T14:06:21.000+01:00	
Recovery Event	2020-12-30T20:01:39.000+01:00	
Recovery Event	2019-02-27T18:55:25.000+01:00	
Recovery Event	2020-03-28T21:26:14.000+01:00	
Recovery Event	2019-12-31T23:03:08.000+01:00	
Recovery Event	2019-03-25T13:37:27.000+01:00	
Recovery Event	2019-02-17T13:21:03.000+01:00	
Recovery Event	2019-10-30T19:12:11.000+01:00	
Carrier Name	No network connection	
Tethering		
Hotspot password required	AndroidAPF91B	

1

1 / 4422

***Slika 25**. Generirani izvještaj u PDF formatu*

6.3 Usporedna analiza obavljenih ekstrakcija na pametnom telefonu

Analiza podataka obavljenih ekstrakcija može se podijeliti na sadržaj uređaja i podatkovne datoteke. Analizirati će se fizička, logička i datotečna ekstrakcija na *Samsung Galaxy EDGE 7* mobilnom uređaju. Logička ekstrakcija ne podržava dohvaćanje podataka kao što su događaji uređaja, korisnici uređaja, lozinke i bežične veze.

U tablici 5. prikazan je broj datoteka za sve tri obavljene ekstrakcije. Iako se većina podataka podudara, postoje razlike dohvaćenih datoteka. Datotečnom ekstrakcijom dohvaćen je jedan kolačić više nego u ostalim ekstrakcijama. Logičkom ekstrakcijom dohvaćeno je 64 instalirane aplikacije, dok je za fizičkom ekstrakcijom dohvaćeno 361 aplikacija, a datotečnom 386 aplikacija. Logičkom ekstrakcijom ne mogu se dohvatiti sve SMS poruke, uključujući i one obrisane.

Tablica 5. *Podaci uređaja*

Ekstrakcija	Logička	Fizička	Datotečna
Podaci uređaja (Obrisane datoteke)			
Automtasko popunjavanje	4	4	4
Kalendar	184 (10)	184 (10)	184 (10)
Popis poziva	4	4	4
Razgovori	5	5	5
Kontakti	7	7	7
Kolačići	341 (1)	341 (1)	342 (1)
Događaji uređaja	X	4	3
Lokacije uređaja	2	2	2
Korisnici uređaja	X	1	1
Preuzimanja	16	16	16
E-mailovi	10 (1)	10 (1)	10 (1)
Instalirane aplikacije	64	361	379
Bilješke	1	1	1
Lozinke	X	383	386
Pretraženi podaci	11	11	11
SMS poruke	11	26 (4)	25 (3)
Korisnički računi	12	15	15
Web oznake	4	4	4
Web povijest	196	196	196
Bežićne mreže	X	2	3

Logičkom ekstrakcijom instaliranih aplikacija dohvaćene su 64 ručno instalirane aplikacije od strane korisnika te unaprijed instalirane aplikacije na samom uređaju. U slučaju fizičke i datotečne ekstrakcije dohvaćen je čak 6 puta veći broj instaliranih aplikacija. Razlog tome je dohvat sistemskih aplikacija Android uređaja koje rade u pozadini. Takve aplikacije su android povratna informacija (engl. *Feedback*), postavke za sigurnost uređaja, lokacija uređaja te slične aplikacije. Logičkom ekstrakcijom ne mogu se dohvatiti obrisane podatkovne datoteke. Usporedba dohvaćenih podatkovnih datoteka za sve tri obavljene ekstrakcije prikazana je u tablici 6.

Tablica 6. *Podatkovne datoteke.*

Ekstrakcija	Logička	Fizička	Datotečna
Podatkovne datoteke (obrisane datoteke)			
Aplikacije	773	4287 (366)	3893
Arhivi	15	84 (54)	28
Audio	42	347 (1)	345
Konfiguracije	X	42	42
Baze podataka	539	653 (6)	647
Dokumenti	6	21	21
Slike	3921	10068 (59)	10161
Tekst	5487	8373 (1058)	7377
Nekategorizirani podaci	11917	20328 (2959)	16767

Fizičkom ekstrakcijom dohvaćeno je najviše datoteka, osim u kategoriji slike. Datotečnom ekstrakcijom dohvaćena je 10161 slika, dok je fizičkom ekstrakcijom dohvaćeno 10068 slika, od kojih je 59 obrisano. Postavljene konfiguracije uređaja ne mogu se dohvatiti logičkom ekstrakcijom, dok je broj dohvaćenih datoteka za fizičku i datotečnu ekstrakciju jednak i iznosi 42 konfiguracije. Najčešće nekategorizirane datoteke su podaci priručne memorije.

7. Zaključak

Razvoj tehnike i tehnologije paralelno je omogućio upotrebnu terminalnih uređaja u čovjekovoj svakodnevnici. Čovjek kao korisnik terminalnih uređaja, među kojima je najraširenija mobilni uređaj, koristi uređaje za širok spektar poslova, zabave i svakodnevnih zadaća. Mobilni uređaj je osmišljen prvotno, kao sredstvo komunikacije na daljinu, ali je razvojem tehnologije postao mnogo više. To svjedočimo u današnjem svijetu, gdje je dodavanjem raznih funkcionalnosti te povezivanjem na bežičnu mrežu mobilni uređaj postao pametni telefon. Kao takav pametni telefon danas se još naziva računalo na dlanu zbog svojih funkcionalnosti te poslova koji se mogu obaviti u stvarnom vremenu na pametnom telefonu, kao i na osobnom računalu.

Razvoj pametnih telefona zajedno sa pripadajućom tehnikom i tehnologijom te neograničene mogućnosti i operacije koje mogu obavljati terminalni uređaji, kako za svakodnevne poslove tako i za nelegalne aktivnosti i kaznena djela. Zbog tih negativnih elemenata i utjecaja čovjeka dolazi do potrebe za digitalnom forenzikom, te naposlijetku za mobilnom forenzikom. Razvoj alata za mobilnu forenziku i analizu podataka omogućio je uvid u sve bitne podatke i datoteke na ispitivanim uređajima, rješavanje jednostavnih dohvata izgubljenih podataka te rješavanje policijski i sudskih istraga.

U diplomskom radu prikazan je postupak ekstrakcije podataka *Google* aplikacija i usluga korištenjem alata za forenzičku analizu *UFED Touch 2*. Prije obavljene ekstrakcije uređaja prikazan je uvid u mobilne uređaje i pametne telefone, funkcionalnosti uređaja, način rada te primjena. U sljedećim poglavljima je objašnjena digitalna forenzika, mobilna forenzika te digitalni dokazi zajedno sa *Google* uslugama i aplikacijama. Prikazane su i objašnjene *Google* aplikacije i usluge na pametnom telefonu nad kojima se provodila ekstrakcija.

Ekstrahirani podaci uređaja analizirani su korištenjem forenzičkog alata za analizu dohvaćenih podataka *UFED Reader*. Analizirani i prikazani rezultati forenzičke analize *Google* usluga i aplikacija na mobilnom uređaju pokazuju potrebu za odabirom odgovarajuće metodologije mobilne forenzike te poštivanje procesa i redoslijed koraka metodologije. Analizirani su podaci tri različite metode ekstrakcije kako bi se dohvatili svi podaci generirani na pametnom telefonu. Svaka od metoda ima svoje prednosti i mane te funkcionalnosti na temelju kojih se odabire odgovarajuća metoda, ovisno o cilju istrage.

Veliki dio analiziranih podatkovnih datoteka i podataka uređaja generirani su i prikupljani od strane *Googleovih* aplikacija i uređaja. Svaki korisnik prije upotrebe aplikacija i uređaja daje privolu za upravljanje podacima trećoj strani. Korisnik upotrebom pametnog telefona i ostalih uređaja te povezivanjem istih na telekomunikacijsku mrežu gubi privatnost. Privatnost i omogućavanje pregleda korisnikovih aktivnosti može se regulirati u postavkama svakog uređaja koji korisnik koristi. Prije upotrebe *Googleovih* usluga i aplikacija te općenito prije upotrebe svih aplikacija i usluga različitih davatelja usluga, potrebno je pročitati pravila o privatnosti i uvijete korištenja. Kao i sve u svakodnevnom životu, tako i korištenje *Google-ovih*

usluga ima svoje prednosti i nedostatke. Prednosti i nedostaci prikazani su forenzičkom analizom u ovom Diplomskom radu. Rezultati analize fizičke ekstrakcije prikazali su najdetaljnije podatke koje prikupljaju uređaj, aplikacije i usluge. Kako bi dobili željeni rezultat potrebno je obaviti više metoda ekstrakcija i odabrati odgovarajuću ovisno o cilju istraživanja.

LITERATURA

[1] Techopedia. Preuzeto sa: https://www.techopedia.com/definition/2977/smartphone [Pristupljeno: travanj 2021.]

[2] Lenovo. Preuzeto sa https://www.lenovo.com/au/en/faqs/pc-life-faqs/what-is-a-smartphone/ [Pristupljeno: travanj 2021.]

[3] Simple Texting. Preuzeto sa https://simpletexting.com/where-have-we-come-since-the-first-smartphone/ [Pristupljeno: travanj 2021.]

[4] Statista. Preuzeto sa https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ [Pristupljeno: travanj 2021.]

[5] Tech Target. Preuzeto sa https://searchmobilecomputing.techtarget.com/definition/mobile-operating-system [Pristupljeno: svibanj 2021.]

[6] Investopedia. Preuzeto sa https://www.investopedia.com/terms/a/android-operating-system.asp [Pristupljeno: svibanj 2021.]

[7] BBC News. Preuzeto sa https://www.bbc.com/news/technology-56639088 [Pristupljeno: Svibanj 2021.]

[8] National Institute of Justice. Preuzeto sa https://nij.ojp.gov/digital-evidence-and-forensics [Pristupljeno: svibanj 2021.]

[9] Tech Terms. Preuzeto sa: https://techterms.com/definition/digital_footprint [Pristupljeno: svibanj 2021.]

[10] Heather Mahalik, Rohit Tamma, Satish Bommisetty. Practical Mobile Forensics, A hands-on guide to mastering mobile forensics for the iOS, Android and Windows Phone platforms, Second Edition. Packt Publishing Ltd. Birmingham, 2016

[11] Homeland Security; TechNote. Preuzeto sa https://www.dhs.gov/sites/default/files/publications/Digital-Forensics-Tools-TN_0716-508.pdf [Pristupljeno: svibanj 2021.]

[12] OpenText. Preuzeto sa https://security.opentext.com/encase-forensic [Pristupljeno: svibanj 2021.]

[13] Oxygen Forensic. Preuzeto sa: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective [Pristupljeno: svibanj 2021.]

[14] Autopsy Digital Forensic: Preuzeto sa https://www.autopsy.com/ [Pristupljeno: svibanj 2021.]

[15] Insectra TS. Preuzeto sa https://www.insectraforensics.com/Cellebrite-Ufed-Touch-Ultimate [Pristupljeno: svibanj 2021.]

[16] TEEL Technologies. Preuzeto sa https://www.teeltech.com/mobile-device-forensic-tools/cellebrite/ufed-touch-ultimate/ [Pristupljeno: svibanj 2021.]

[17] TEEL Technologies. Preuzeto sa: https://teeltech.com/mobile-device-forensic-tools/cellebrite/ufed-touch-logical/ [Pristupljeno: svibanj 2021.]

[18] Cellebrite. Preuzeto sa: https://www.cellebrite.com/en/cellebrite-introduces-ufed-touch2-platform/ [Pristupljeno: svibanj 2021.]

[19] Oleg Skulkin, Donnie Tindall, Rohit Tamma. Learning Android Forensics, Analyze Android devices with the latest forensic tools and techniques ;Second Edition. Packt Publishing Ltd., 2018

[20] Minterest. Preuzeto sa: https://www.matrics360.com/google-products-and-services/ [Pristupljeno: svibanj 2021.]

[21] Website Builder : Preuzeto sa https://websitebuilder.org/blog/google-stats/ [Pristupljeno: rujan 2021.]

[22] Statista : Preuzeto sa:https://www.statista.com/topics/1001/google/#dossierKeyfigures [Pristupljeno: ožujak 2022.]

[23] Google: Preuzeto sa: https://about.google/products/ [Pristupljeno: studeni 2021.]

[24] Avast: Preuzeto sa: https://www.avast.com/c-how-google-uses-your-data/ [Pristupljeno: Veljača 2022.]

[25] Boldist: Preuzeto sa: https://boldist.co/analytics/google-data-collection/ [Pristupljeno: ožujak 2022.]

[26] Heather Mahalik, Rohit Tamma, Satish Bommisetty. Practical Mobile Forensics, Forensically investigate and analyze iOS, Android and Windows 10 devices; Fourth Edition. Packt Publishing Ltd. Birmingham, April 2020.

[27] The Forensic Process Analysis of Mobile Device, Dasari Manendra Sai1, Nandagiri R G K Prasad2, Satish Dekka, 3, International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015

[28] Chuck Easttom. An in-depth guide to mobile device forensics, First Edition, Crc Press, 2022

[29] Study.com: Preuzeto sa: https://study.com/academy/lesson/mobile-device-forensics-tool-classification-system-definition-levels.html [Pristupljeno: Svibanj 2022.]

[30] Infosec: Preuzeto sa: https://resources.infosecinstitute.com/topic/mobile-forensics-process-steps-types/ [Pristupljeno: Svibanj 2022.]

[31] Cellebrite.com: Preuzeto sa: https://cellebrite.com/en/selective-file-system-extraction-in-cellebrite-ufed/ [Pristupljeno: svibanj 2022.]

[32] Android Forensic Chapter 3- Data Extraction with Universal Forensic Extraction Device (UFED): Preuzeto sa: https://content-calpoly-edu.s3.amazonaws.com/cci/1/documents/ccic_forensics_manual/Android%20Forensics%20Chapter%203%20-%20Data%20Extraction%20with%20Universal%20Forensic%20Extraction%20Device%20%28UFED%29.pdf [Pristupljeno: svibanj 2022.]

[33] Autorizirana predavanja: Forenzička analiza informacijsko komunikacijskog sustava: Metode ekstrakcije podataka mobilnih uređaja, Fakultet prometnih znanosti. Preuzeto sa: https://moodle.srce.hr/2020-2021/pluginfile.php/4819602/mod_resource/content/1/Metode%20ekstrakcije%20podataka%20mobilnih%20ure%C4%91aja.pdf [Pristupljeno: Svibanj 2022.]

[34] Developers.android.com: Preuzeto sa https://developer.android.com/studio/command-line/adb [Pristupljeno: Lipanj 2022.]

[35] Support.google.com: Preuzeto sa https://support.google.com/googleplay/android-developer/answer/6048248?hl=en [Pristupljeno: Lipanj 2022.]

[36] CookieYes.com: Preuzeto sa https://www.cookieyes.com/blog/tracking-cookies/

[Pristupljeno: Srpanj 2022.]

[37] IBM.com: Preuzeto sa https://www.ibm.com/docs/en/i/7.4?topic=files-data-source [Pristupljeno: Srpanj 2022.]

[38] The evolution of The Smartphone: Preuzeto sa https://storymaps.arcgis.com/stories/43449bc48bbc4937b440e9ed3e2ea11c [Pristupljeno: Srpanj 2022.]

[39] Gs.statcounter.com: Preuzeto sa: https://gs.statcounter.com/vendor-market-share/mobile/worldwide/#yearly-2016-2022-bar [Pristupljeno: Srpanj 2022.]

[40] Bankmycell.com: Preuzeto sa: https://www.bankmycell.com/blog/ [Pristupljeno: srpanj 2022.]

[41] Statista.com Preuzeto sa: https://www.statista.com/statistics/566069/predicted-number-of-smartphone-users-in-croatia/ [Pristupljeno: kolovoz 2022.]

[42] Nelson B, Phillips A, Steaurty C: Guide to Computer forensics and investigations, SAD, 2018.

[43] Majić, P. Usporedni prikaz za postupak forenzičke analize sustava bespilotnih zrakoplova. Fakultet prometnih znanosti, Zagreb, 2021

[44] Sleuthkit.com: Preuzeto sa: https://www.sleuthkit.org/autopsy/ [Pristupljeno: Srpanj 2022.]

[45] Statista.com: Preuzeto sa https://www.statista.com/statistics/1156150/leading-google-search-queries-croatia/ [Pristupljeno: Srpanj 2022.]

[46] Delija D. Remote digital forensics practices. *International Journal of DIGITAL TECHNOLOGY & ECONOMY*. 2017;2(1): 27 – 36

[47] Ćosić Z., Ćosić J., Bača M. Biometric System Vulnerability as a Compromising Factor for Integrity od Chain of Custody and Admissibility of Digital Evidence in Court of Justice: Analysis and Improvement Proposal. 2014; 38(1): 11-33

[48] Zareen A. & Baig S. (2010). Notice of Violation of IEEE Publication Principles Mobile Phone Forensics: Challenges, Analysis and Tools Classification. 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensics Engineering. Preuzeto sa: https://ieeexplore.ieee.org/abstract/document/5491956 [Pristupljeno: srpanj 2022.]

[49] Alhassan J., Misra S., Adewumi A., Oguntoye R. T., Maskeliunas R., Damaševičius R. Comparative Evaluation of Mobile Forensics Tools. Advences in Intelligent Systems and Computing. 2018, 105-114.

Popis kratica

ADB (*Android Debug Bridge*) programski alat koji se koristi za otklanjanje pogrešaka na uređajima koji se temelje na Androidu

API (*Application programming interface*) aplikacijsko programsko sučelje

CPU (*Central processing unit*) središnja procesorska jedinica

FTK (*AccessData's Forensic Toolkit*) računalni forenzički softver izrađen u programu AccessData

GPS (*Global Positioning System*) sustav za navigaciju

GUI (*Graphical user interface*) grafičko korisničko sučelje

IBM (*International Business Machines*) Američka multinacionalna tehnološka korporacija

ID (*Identify document*) identifikacijski dokument

IOT (*Internet of things*) internet stvari

IP (*Internet Protocol*) internet protokol

JPEG (*Joint Photographic Experts Group*) Standard kompresije slike

MD5 (message-digest) Algoritam za autentifikaciju poruka

MP3 (*Moving Picture Experts Group Layer-3 Audio*) Format za kodiranje digitalnog zvuka

OS (*Operating system*) operativni sustav

OGG (*Open-source file format for multimedia)* Format datoteke otvorenog koda za multimediju

SANS (*Escal Instiute of Advanced Technologies*) SANS institut

SD (*Secure Digital*) Memorijska kartica

SIM (*Subscriber Identity Module*) modul na kojem je pohranjen unikatni broj kojim se identificira pretplatnik na mobilnoj telefonskoj mreži

SMS (*Short Message Service*) usluga je slanja kratkih tekstualnih poruka unutar GSM standarda mobilne telefonije

SPC (*Simon Personal Communicator*) uređaj sa zaslonom osjetljivim na dodir

UFED (*Universal Forensic Extraction Device*) Univerzalni uređaj za forenzičku ekstrakciju

USB (Universal Serial Bus) univerzalna serijska sabirnica

WEBP (*Web Picture Format*) Format web slike

Popis slika

Slika 1. Broj korisnika pametnih telefona u svijetu, [4]. 5
Slika 2. Zastupljenost mobilnih OS-a u svijetu u periodu od 2016. do 2021. godine,[5]. 7
Slika 3. UFED Touch2 Ultimate komplet,[16] 16
Slika 4. UFED Touch2 radna jedinica, [18] 17
Slika 5. Datoteke i podaci Android aplikacija,[19]. 18
Slika 6. Google Chrome podatci,[19]. 19
Slika 7. Dio dostupnih Google usluga,[20] 20
Slika 8. Najtraženiji pojmovi u 2021.godini, [22] 21
Slika 9. Najtraženiji pojmovi na Google tražilici u Republici Hrvatskoj prema indeks vrijednosti, [44]. 22
Slika 10. Metode ekstrakcije podataka mobilnih uređaja, [28] 30
Slika 11. Android Debugging bridge i Developer options 33
Slika 12. Automatsko prepoznavanje mobilnog uređaja, UFED Touch 2 34
Slika 13. Ekstrakcija podataka s mobilnog uređaja 34
Slika 14. Podaci o uređaju generirani u Cellebrite Reader alatu 36
Slika 15. Grupiranje podataka nakon ekstrakcije. 37
Slika 16. Prikaz događaja uređaja u Cellebrite Reader alatu 37
Slika 17. Automatsko popunjavanje ključnih riječi. 38
Slika 18. Usporedba pohranjenih kolačića na domeni google.com 38
Slika 19. Podaci u aplikaciji Google kalendar 39
Slika 20. Google Hangouts aplikacija. 39
Slika 21. Slike pohranjene u memoriji terminalnog uređaja 40
Slika 22. Prikaz zvučnog zapisa u Cellebrite Reader alatu 41
Slika 23. Prikaz baze podataka i heksadekadski zapis web stranice 42
Slika 24. Generiranje izvještaja u UFED Reader alatu 42
Slika 25. Generirani izvještaj u PDF formatu 43

Popis tablica

Tablica 1. Upotreba pametnih telefona u svijetu,[40]. 6
Tablica 2. Usporedba značajki forenzičkih alata, [42] 13
Tablica 3. Značajke forenzičkih alata za analizu podataka,[42],[43] 15
Tablica 4. Usporedba funkcionalnosti UFED Touch 2 alata,[31] 17
Tablica 5. Podaci uređaja..... 44
Tablica 6. Podatkovne datoteke. 45

Popis grafikona

Grafikon 1. Tržišni udio dobavljača pametnih telefona u svijetu za razdoblje 2016.-2022., [39] 4
Grafikon 2. Broj korisnika pametnih telefona u Hrvatskoj u milijunima (2015-2022), [40] 6
Grafikon 3. Broj preuzimanja aplikacija u 6. mjesecu 2021. godine u milijunima,[22] 24

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom **Forenzika pametnog telefona temeljena na podacima Google usluga** , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 3.9.2022. Ivan Grgić
(ime i prezime, *potpis*)