Forenzička analiza pametnog Android telefona

Barišić, Ivan

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

FORENZIČKA ANALIZA PAMETNOG ANDROID TELEFONA

FORENSIC ANALYSIS OF AN ANDROID SMARTPHONE

Mentor: doc. dr. sc. Ivan Cvitić

Student: Ivan Barišić

JMBAG: 0135254850

Zagreb, kolovoz 2023.

SAŽETAK

Pametni telefoni, posebice oni koji koriste Android operativni sustav, postali su integralni dio modernog života, služeći mnogo više od osnovne svrhe komunikacije. Sa svakom interakcijom, ovi uređaji akumuliraju obilje informacija, od dokumentiranja osobnih poruka do praćenja lokacija korisnika. Ovaj rad pruža detaljan uvid u kompleksnu arhitekturu Android sustava, naglašavajući ključne komponente i sigurnosne protokole koji oblikuju osnovu forenzičke analize. Uz upotrebu specifičnih alata, kao što su ADB i drugi, istražujemo metode ekstrakcije i analize podataka s Android uređaja. Kroz ovaj pristup, rad naglašava kritičnu važnost razumijevanja kako ovi uređaji pohranjuju i upravljaju podacima te kako stručnjaci mogu iskoristiti te informacije u forenzičke svrhe.

KLJUČNE RIJEČI: Android arhitektura; forenzička analiza; ekstrakcija podataka; digitalni tragovi; ADB alat.

SUMMARY

Smartphones, especially those running the Android operating system, have become an integral part of modern life, serving much more than the basic purpose of communication. With every interaction, these devices accumulate a wealth of information, from documenting personal messages to tracking user locations. This paper provides an in-depth insight into the complex architecture of the Android system, highlighting key components and security protocols that form the foundation of forensic analysis. Using specific tools such as ADB and others, we explore methods of extracting and analyzing data from Android devices. Through this approach, the work emphasizes the critical importance of understanding how these devices store and manage data and how professionals can leverage this information for forensic purposes.

KEYWORDS: Android architecture; forensic analysis; data extraction; digital traces; ADB tool.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 22. svibnja 2023.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 7063

Pristupnik: **Ivan Barišić (0135254850)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Forenzička analiza pametnog Android telefona**

Opis zadatka:

Završnim radom potrebno je prikazati arhitekturu sutava Android te procese i postupke provedbe forenzilke analize pametnih telefona. Potrebno je prikazati dostupne alate za forenzičku analizu Android uređaja te provesti ekstrakciju i analizu podataka pametnog telefona.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za završni ispit:

Sadržaj

1. Uvod

U doba brzog tehnološkog napretka i digitalizacije, mobilni pametni uređaji postali su neizostavni aspekt modernog života. Uz njihovu sveprisutnost, ovi pametni uređaji postali su ključni izvor informacija u raznim istraživanjima, uključujući i forenzičku analizu digitalnih tragova.

Forenzička analiza Android uređaja pruža dubok uvid u podatke pohranjene na tim uređajima, uključujući povijest poziva, tekstualne poruke, e-mailove, fotografije, videozapise i mnoge druge informacije koje su od ključne važnosti u sudskim sporovima, kriminalističkim istragama i digitalnoj forenzici općenito. Razumijevanje arhitekture sustava Android i metoda forenzičke analize pametnih telefona je od presudne važnosti za forenzičke stručnjake.

Svrha ovog završnog rada jest istražiti i analizirati procese ekstrakcije i analize podataka s Android uređaja, koristeći se javno dostupnim alatima i tehnikama. Cilj je pružiti pregled metodologije i prakse forenzičke analize pametnih telefona na Android platformi. Naslov završnog rada je: Forenzička analiza pametnog Android telefona. Rad je podijeljen u sedam cjelina:

1. Uvod
2. Arhitektura sustava Android
3. Forenzička analiza pametnih telefona
4. Alati za forenzičku analizu Android uređaja
5. Ekstrakcija podataka Android uređaj
6. Analiza ekstrahiranih podataka i izvještaj
7. Zaključak

Drugo poglavlje detaljno razmatra temelje i komponente Android sustava. Prikazuje se sigurnost sustava, kernela i aplikacija na Android platformi. Poseban naglasak stavlja se na strukturu datotečnog sustava Android uređaja te se ističe važnost razumijevanja arhitekture za temeljitu i učinkovitu forenzičku analizu Android uređaja.

Forenzička analiza pametnih telefona se fokusira na metodologije i prakse koje su specifične za forenzičku analizu pametnih telefona. Razmatraju se izazovi, postupci i specifičnosti forenzičke analize u kontekstu mobilnih uređaja.

U četvrtom poglavlju opisuju se kriteriji temeljem kojih se biraju odgovarajući alati za forenzičku analizu Android uređaja. Daje se pregled popularnih alata dostupnih na tržištu, s posebnim osvrtom na besplatne i otvorene alate.

Ekstrakcija podataka Android uređaja detaljno opisuje proces pripreme Android uređaja za ekstrakciju podataka. Glavni naglasak stavlja se na ekstrakciju podataka koristeći Android Debug Bridge (ADB), jedan od ključnih alata za pristup podacima na uređaju.

Nakon ekstrakcije podataka, šesto poglavlje pristupa analizi tih podataka. Prikazuje se analiza podataka dobivenih iz aplikacija te direktno dostupnih podataka s uređaja. Diskutira se o tome kako interpretirati ekstrahirane podatke.

2. Arhitektura sustava Android

Android je skup softvera otvorenog koda (engl. *Android Open Source Project*, AOSP) stvoren za širok raspon uređaja s različitim faktorima oblika, što ga čini iznimno prilagodljivim za različite potrebe i zahtjeve tržišta. Glavni cilj Androida je stvoriti platformu koja će biti otvorena za operatere, proizvođače originalne opreme (engl. *Original Equipment Manufacturer*, OEM) i razvojne programere, omogućujući im da svoje inovativne ideje pretvore u stvarnost i predstave proizvode koji će unaprijediti mobilno iskustvo korisnika diljem svijeta, [1].

Otvoreni pristup Android platformi potiče suradnju i razmjenu znanja među različitim dionicima industrije, bez centralne točke kontrole ili ograničenja inovacija. To rezultira raznolikošću uređaja i aplikacija koje korisnicima omogućuju prilagodbu i personalizaciju prema njihovim željama i potrebama. Bilo da se radi o pametnim telefonima, tabletima, televizorima, automobilima ili drugim pametnim uređajima, Android pruža konzistentno i integrirano korisničko iskustvo, [1].

Jedinstvena karakteristika Androida je njegov otvoreni izvorni kod, koji omogućuje prilagodbu i nadogradnju sustava prema potrebama proizvođača i korisnika. Programeri mogu pristupiti izvornom kodu i prilagoditi ga svojim potrebama, stvarajući tako prilagođena rješenja i inovativne aplikacije koje poboljšavaju korisničko iskustvo. Takav pristup omogućuje i bolju sigurnost sustava, jer velika zajednica razvijatelja surađuje na otkrivanju i rješavanju sigurnosnih ranjivosti. Otvoreni izvorni kod također potiče brže inovacije i razvoj, jer se novi koncepti i tehnologije lako integriraju u platformu, [2].

Duboko razumijevanje Android ekosustava, uključujući sigurnosne protokole, strukturu datotečnih sustava, upravljanje aplikacijama i ostale specifične značajke, ključno je za provođenje učinkovite forenzičke istrage. Bez temeljite pozadine ove vrste, stručnjak za forenziku može propustiti ključne podatke ili donijeti netočne zaključke.

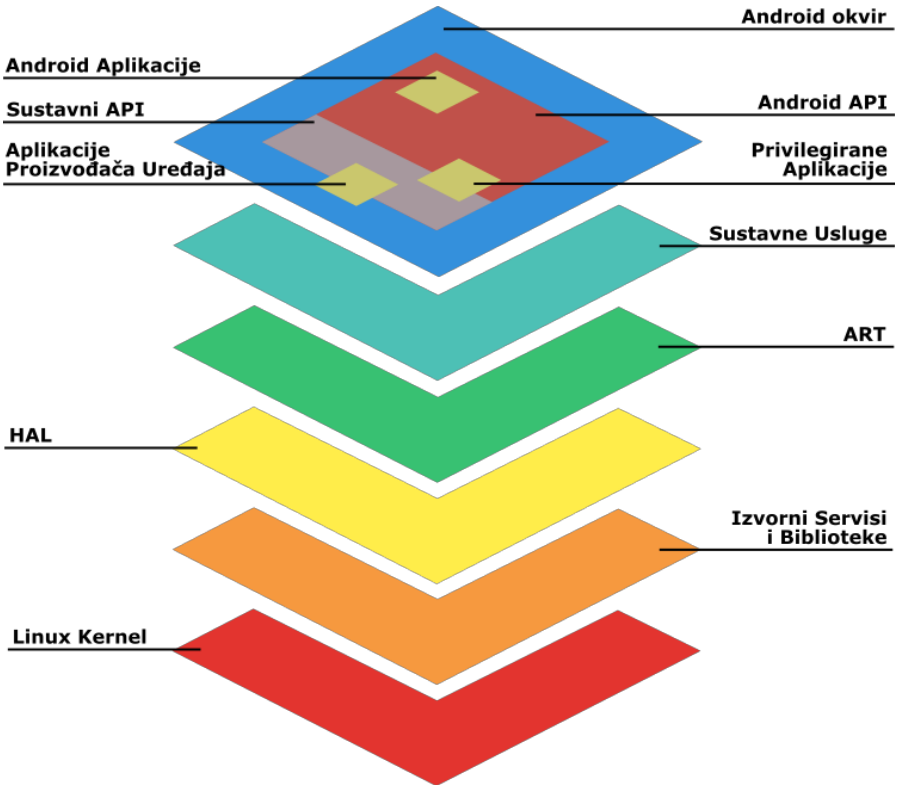
Stjecanje znanja o tim temeljima nije samo korisno, već i neophodno. Osim što omogućuje stručnjaku da donosi informirane i precizne odluke tijekom istrage, također pomaže u izradi i implementaciji učinkovitih strategija za izdvajanje, analizu i interpretaciju podataka. Uz to, duboko razumijevanje Android ekosustava može omogućiti forenzičaru da brže identificira potencijalne izvore dokaza, preciznije interpretira podatke i anticipira moguće izazove ili prepreke tijekom istrage, [3].

2.1. Temelji i komponente Android sustava

Za učinkovito razumijevanje forenzičkih koncepta prilikom rada s Androidom, potrebno je posjedovati osnovno razumijevanje arhitekture Androida. Kao i kod računala, svaki računalni sustav koji interagira s korisnikom i izvršava složene zadatke, zahtijeva operativni sustav za

efikasno upravljanje tim zadacima. Operativni sustav, bilo da se radi o sustavu za stolna računala ili mobilne uređaje, zadužen je za upravljanje resursima sustava te pruža način za interakciju aplikacija s hardverom ili fizičkim komponentama u svrhu obavljanja određenih zadataka.

Kao i bilo koja druga platforma, Android se sastoji od slojeva koji se izvršavaju jedan iznad drugog. Preduvjet razumijevanja ekosustava Android operativnog sustava predstavlja osnovno razumijevanje kasnije spomenutih slojeva i njihovih funkcija.



Slika 1. AOSP arhitektura,
Izvor: [4]

Svaki od ovih slojeva, prikazanih sa slikom 1, obavlja nekoliko operacija koje podržavaju specifične funkcije operativnog sustava. Svaki sloj pruža usluge slojevima koji se nalaze iznad njega:

- **Android aplikacija,** je softver kreiran pomoću Android programskog sučelja (engl. *Application Programming Interface*, API). Iako je Google Play trgovina najpoznatiji izvor za preuzimanje ovih aplikacija, postoje i druge alternative. Neke aplikacije mogu biti unaprijed instalirane na uređajima kako bi podržale njihove osnovne funkcije. U kontekstu forenzičke analize, podaci iz aplikacija kao što su datoteke, logovi i baze podataka mogu pružiti ključne informacije o korisnikovim aktivnostima i navikama, [4].
- **Privilegirana aplikacija,** razvija se kombinacijom Android i sustavnih API-ja, te je nužno da bude unaprijed instalirana na uređaju s odgovarajućim privilegijama. Ovim aplikacijama dopušteno je izvršavati radnje koje mogu značajno utjecati na sustav,

poput promjene sustavskih postavki ili kontrole drugih aplikacija. U forenzičkoj analizi, one su posebno relevantne zbog mogućnosti pristupa i manipulacije osjetljivim podacima te praćenja sistemskih aktivnosti, [4].

- **Aplikacija proizvođača uređaja,** kombiniraju Android i sustavne API-je s izravnim pristupom Android okvira. Zbog pristupa specifičnim nestabilnim API-ima, one su unaprijed instalirane i ažuriraju se isključivo uz nadogradnju sustava uređaja. Primjerice, aplikacije poput Samsung Health ili Huawei Music rezervirane su za uređaje njihovih proizvođača i često su duboko integrirane u Android sustav. U forenzičkom kontekstu, njihova bliska integracija i moguć pristup osjetljivim podacima čine ih posebno značajnima za analizu, [4].
- **Sustavni API,** specifični Android API-ji dostupni isključivo partnerima i OEM proizvođačima za integraciju u predinstalirane aplikacije. Omogućuju aplikacijama pristup osnovnim funkcionalnostima operativnog sustava, uključujući mrežnu komunikaciju, upravljanje datotekama, interakciju sa zaslonom na dodir i drugih, [4].
- **Android API,** javno dostupno programsko sučelje namijenjeno razvoju aplikacija za Android platformu. Omogućuje programerima kreiranje aplikacija kompatibilnih s Android uređajima, [4].
- **Android okvir (engl. *Android framework*),** u Android arhitekturi postavljen iznad sustavskih usluga, djelujući kao posrednik između operativnog sustava i aplikacija. Omogućuje programerima kreiranje korisničkih sučelja, upravljanje aplikacijama, interakciju s hardverom te uključuje ključne komponente kao što su upravljanje interakcijama korisnika (engl. *Activity*), dugotrajne operacije u pozadini (engl. *Service*), upravljanje podacima aplikacija (engl. *Content Provider*) i distribuciju i obradu sistemskih i aplikacijskih poruka (engl. *Broadcast Receiver*), [4].
- **Sustavne usluge (engl. *System services*),** komponente u Androidu koje omogućavaju aplikacijama interakciju s hardverom uređaja. Aktiviraju se kroz Android okvir API i služe kao posrednik između aplikacijskog softverskog koda i fizičke opreme uređaja, [4].
- **Android runtime (ART),** predstavlja ključni sloj unutar Android arhitekture i služi kao okruženje za izvršavanje i pokretanje Android aplikacija. ART izvodi prijevod bajt-koda aplikacije u instrukcije specifične za procesor koje izvršava izvršno okruženje uređaja, [4].
- **Sloj apstrakcije hardvera (engl. *Hardware Abstraction Layer*, HAL),** sloj unutar Android arhitekture koji pruža standardizirano sučelje za komunikaciju Androida s hardverom uređaja. Omogućuje proizvođačima da integriraju svoje drivere, osiguravajući da Android sustav ostane neovisan o specifičnim implementacijama drivera, te omogućava adaptaciju funkcionalnosti bez mijenjanja viših razina sustava, [4].

- **Izvorni servisi i biblioteke (engl. *Native daemons and libraries*),** sloj koji uključuje niz izvornih servisa poput upravljanja medijima, površinom i multimedijalnim datotekama. Ovi servisi, poznati kao "daemon", rade u pozadini, omogućujući aplikacijama pristup hardverskim resursima uređaja na efikasan način bez potrebe za interakcijom s korisnikom, [4].
- **Linux Kernel,** središnji je dio Android operativnog sustava koji upravlja osnovnim funkcijama poput upravljanja procesima, memorijom i sigurnošću. Android koristi Linux kao temelj zbog njegove dokazane sigurnosti i upravljačkih sposobnosti. Svaka verzija Androida temelji se na specifičnoj verziji Linux kernela, [3], [4].

2.2. Sigurnost sustava, kernela i aplikacija na Androidu

Android je platforma dizajnirana s ključnim fokusom na sigurnost, pružajući višeslojnu zaštitu korisničkih podataka na mobilnim uređajima. Ove značajke sigurnosti, ugrađene izravno u arhitekturu platforme, imaju trostruki cilj: zaštitu korisničkih podataka, zaštitu sistemskih resursa i osiguranje da jedna aplikacija ne može pristupiti podacima druge aplikacije, [2].

Android istovremeno pruža razvojnoj zajednici mogućnosti za izgradnju sigurnih aplikacija kroz određene sigurnosne alate i postavke. Međutim, ove složene značajke sigurnosti mogu ponekad otežati forenzičkim istražiteljima pristup potrebnim podacima. Stoga je za forenzičke istražitelje ključno razumijevanje unutarnje strukture sigurnosti Androida kako bi se identificirale najbolje metode i tehnike koje se mogu primijeniti u određenim situacijama, kao i shvatiti tehnička ograničenja tih tehnika, [3].

2.3. Struktura datotečnog sustava na Android uređajima

Glavni cilj forenzičke analize je ekstrakcija relevantnih podataka iz uređaja. Stoga, za uspješnu forenzičku analizu, ključno je imati temeljno razumijevanje vrste podataka koji se pohranjuju na uređaju, njihove lokacije, načina pohrane te detalja o datotečnim sustavima na kojima se podaci nalaze. To znanje igra iznimno važnu ulogu za forenzičke analitičare jer im omogućuje informiranu odluku o tome gdje potražiti podatke i koje tehnike primijeniti za njihovo ekstrahiranje.

2.3.1. Izgled Android particije

Android uređaji koriste particioniranje, logičko dijeljenje trajne memorije, kako bi učinkovito organizirali vitalne podatke i aplikacije potrebne za rad uređaja. Svaka particija ima specifičnu funkciju i sadrži različite vrste podataka, što omogućava logičnu i nezavisnu upotrebu svake sekcije.

Uobičajene particije uključuju, [5]:

- BOOT: Ključna za pokretanje uređaja, sadržava informacije potrebne za inicijalno pokretanje, uključujući kernel.
- CACHE: Privremeno skladišti često korištene podatke kao što su logovi za oporavak i paketi ažuriranja.
- RECOVERY: Omogućuje pokretanje uređaja u konzoli za oporavak, koristan za ažuriranje sustava ili vraćanje na tvorničke postavke.
- SYSTEM: Sadrži ključne komponente Android OS-a, uključujući Android okvir i prethodno instalirane aplikacije.
- USERDATA: Glavno skladište za korisničke podatke poput aplikacija, postavki, medija i dokumenata.

Razumijevanje ovih particija bitno je za tehničko razumijevanje Android uređaja i za pristupe poput forenzičke analize.

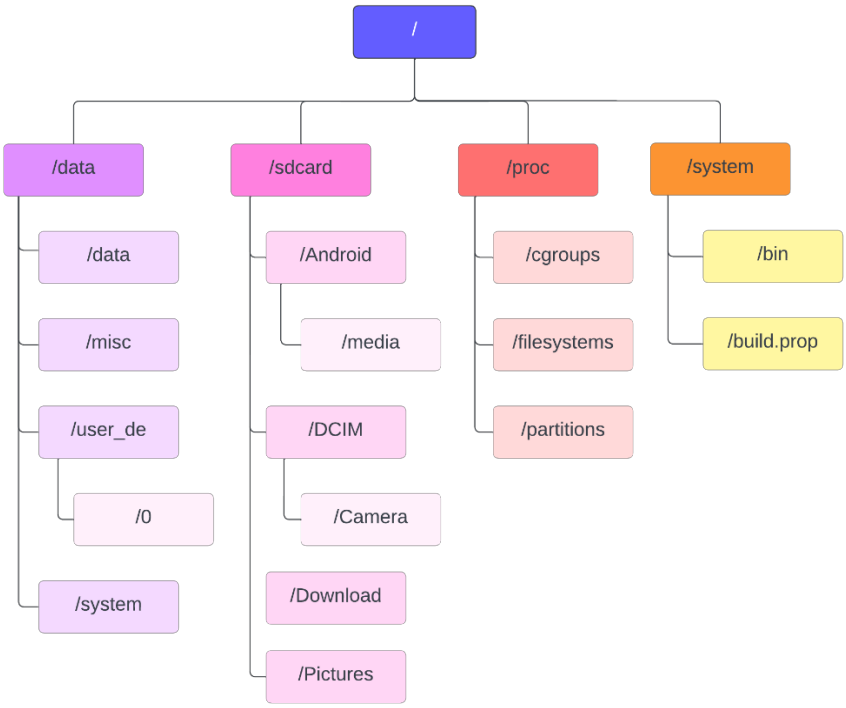
2.3.2. Android hijerarhija datoteka

Za uspješnu forenzičku analizu na Android sustavu ključno je razumijevanje njegove hijerarhije datoteka. Androidova hijerarhija temelji se na Unix-sličnim operativnim sustavima, naročito Linuxu. Glavna karakteristika ove hijerarhije je korijenski direktorij označen znakom "/", koji služi kao početna točka za sve ostale datoteke i direktorije, prikazano slikom 2., [5].

Sve datoteke i direktoriji na Androidu smješteni su unutar ove hijerarhije. Ova organizacija datoteka je centralna za operativni sustav, pružajući strukturirano mjesto za sve, od sustavskih datoteka do korisničkih podataka.

Iako Androidova hijerarhija datoteka slijedi osnovnu strukturu Linuxa, proizvođači uređaja mogu unijeti manje izmjene, što znači da se struktura može neznatno razlikovati ovisno o uređaju i verziji Androida.

Za pristup cijeloj hijerarhiji potreban je root pristup. Ovaj pristup omogućuje korisnicima da pristupaju svim datotekama i direktorijima, uključujući one koji su inače skriveni ili zaštićeni, [5].



Slika 2. Hijerarhija ključnih direktorija

2.3.3. Pohrana podataka aplikacije na uređaju

Android uređaji pohranjuju obilje osjetljivih informacija putem različitih aplikacija. Za bolje razumijevanje, aplikacije se mogu klasificirati u četiri glavne kategorije, [5]:

1. Standardne aplikacije uključene u Android operativni sustav
2. Aplikacije instalirane od strane proizvođača uređaja
3. Aplikacije dodane od strane pružatelja mobilnih usluga
4. Aplikacije koje su korisnici instalirali samostalno

Svaka od ovih kategorija aplikacija generira i pohranjuje specifične vrste podataka na uređaju. Ovi podaci mogu biti ključni za forenzičku analizu jer često sadrže važne informacije relevantne za istragu. Primjeri vrsta podataka koji se mogu pronaći na Android uređaju uključuju, [5]:

- SMS i MMS poruke
- Poruke razgovora
- Sigurnosne kopije podataka
- E-mail poruke
- Povijest poziva
- Kontakti
- Fotografije i videozapisi
- Povijest internetskog pregledavanja

- GPS podaci
- Preuzete datoteke i dokumenti
- Podaci povezani s instaliranim aplikacijama (poput Facebooka, Twittera i drugih društvenih mreža)
- Podaci o događanjima u kalendaru.

Podaci se mogu pohranjivati na dva načina: interno ili eksterno. U slučaju eksterne pohrane, poput SD kartice, podaci se mogu smjestiti na bilo koju lokaciju. Međutim, kod interne pohrane, lokacija je unaprijed definirana. Svi podaci aplikacija na uređaju, bilo da se radi o sistemskim ili korisnički instaliranim, automatski se pohranjuju u poddirektorij /data/data, koji je imenovan prema paketu aplikacije. Na primjer, podaci standardne Android e-mail aplikacije s imenom paketa com.android.email pohranjeni su na lokaciji /data/data/com.android.email. Detaljnija rasprava o ovom konceptu bit će u nadolazećim segmentima, [5].

2.4. Značaj razumijevanja arhitekture za forenzičku analizu Android uređaja

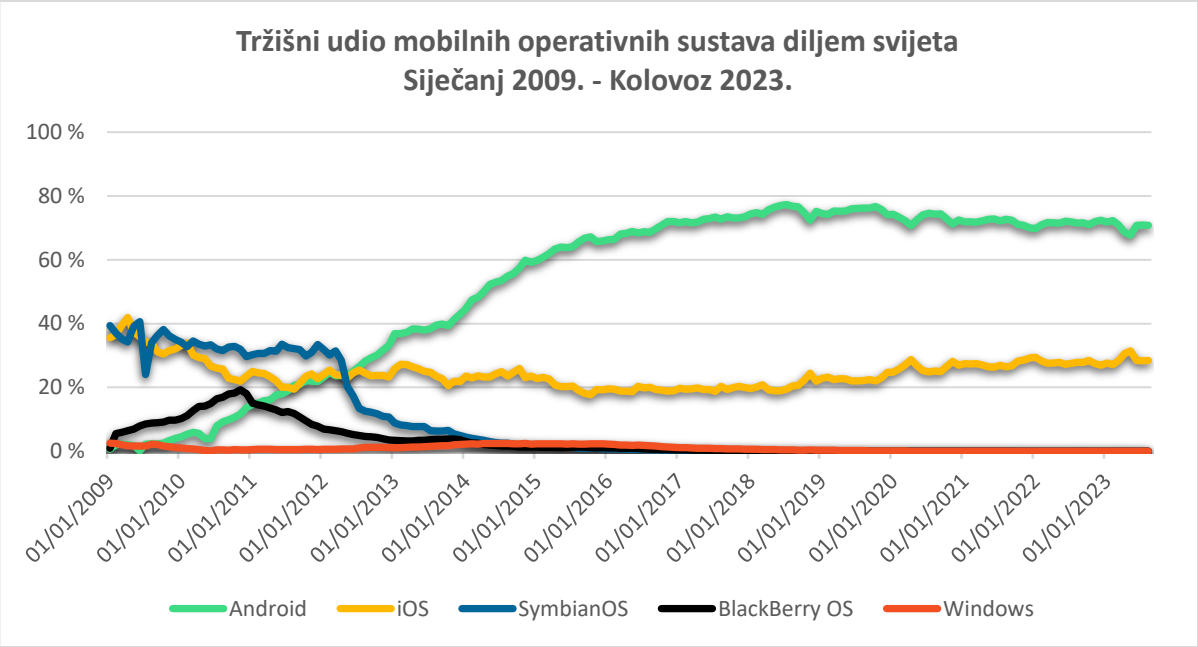
Struktura datotečnog sustava, organizacija particija memorije, funkcionalnost aplikacija i servisa, sustav prava pristupa te sigurnosni protokoli predstavljaju aspekte Android arhitekture koji imaju suštinsku važnost za forenzičke analitičare, [3]:

- Androidov datotečni sustav reflektira Linux nasljeđe. Direktoriji su hijerarhijski organizirani, što omogućava identifikaciju lokacija datoteka.
- Memorija je podijeljena u particije poput BOOT, SYSTEM, i DATA. Svaka pohranjuje specifične podatke, a njihovo razumijevanje omogućava efikasan pristup informacijama.
- Aplikacije variraju od prethodno instaliranih do korisnički dodanih. Sve generiraju podatke koji mogu biti relevantni za analizu.
- Prava pristupa reguliraju koji korisnici i procesi mogu pristupiti kojim podacima, utječući na mogućnosti analize.
- Sigurnosni protokoli, poput enkripcije, mogu predstavljati izazov, ali njihovo razumijevanje omogućava efikasniju analizu.

Svaki od ovih aspekata arhitekture Android uređaja može značajno utjecati na forenzičku analizu. Bez dubinskog razumijevanja ovih aspekata, postoji rizik da forenzičari neće biti u stanju locirati ili pristupiti relevantnim podacima. Iz tog razloga, duboko razumijevanje arhitekture Android uređaja predstavlja nužnost za temeljitu i efikasnu forenzičku analizu.

3. Forenzička analiza pametnih telefona

Kada se govori o mobilnoj forenzici, posebno u kontekstu Android uređaja, neophodno je prilagoditi se i održati korak sa stalnim inovacijama i promjenama koje se događaju. Android je postao najzastupljeniji mobilni operativni sustav tijekom 2012. Godine kao što vidimo u grafu 1. Pored brzih ažuriranja i izdanja novih verzija operativnih sustava, aplikacije se stalno ažuriraju, mijenjaju načine na koje pohranjuju i upravljaju podacima, uključujući i mjere zaštite privatnosti korisnika. Ove promjene mogu značajno utjecati na pristup, ekstrakciju i interpretaciju podataka.



Graf 1. Tržišni udio operativnih sustava diljem svijeta
Izvor: [6]

Forenzičari moraju biti u toku s tim promjenama, prilagođavajući svoje metode i alate kako bi ostali učinkoviti u svom radu. To uključuje stalno usavršavanje, obuku i istraživanje najnovijih razvojnih trendova i tehnika u industriji. Bez ove prilagodbe, forenzičari se suočavaju s rizikom da neće moći u potpunosti i pravilno analizirati podatke s najnovijih uređaja, što može dovesti do nepotpunih ili netočnih zaključaka, [7].

Iako stvaranje univerzalnih standarda može biti teško u takvom okruženju, važno je uspostaviti neke osnovne principe i prakse koje mogu pružiti vodstvo forenzičarima. To uključuje princip dobro dokumentiranih i reproducibilnih postupaka, princip ne izmijenjenosti dokaza, kao i obvezu neprekidnog obrazovanja i profesionalnog razvoja, [7].

3.1. Digitalna forenzička analiza

Digitalna forenzika predstavlja segment forenzičke znanosti fokusiran na identifikaciju, prikupljanje, interpretaciju i prezentaciju podataka pohranjenim na računalima, digitalnim uređajima ili drugim medijima za digitalnu pohranu. Elektronički dokazi obuhvaćaju informacije sačuvane na uređajima kao što su prijenosna računala, pametni telefoni, digitalni snimači, bespilotne letjelice, GPS uređaji te igraće konzole. Cilj digitalne forenzike jest konverzija ovih podataka u informacije relevantne za pravosudne postupke, uz osiguranje da je pristup tim informacijama proveden koristeći standardizirane forenzičke tehnike, čime se osigurava njihova pravosudna prihvatljivost, [8].

Digitalna forenzika vezana uz Android uređaje odnosi se na analizu podataka sačuvanih na uređajima koji koriste Android operativni sustav. Zbog različitih proizvođača, modela i verzija Androida, kao i specifičnih aplikacija koje korisnici instaliraju, ovaj segment forenzike nudi određene izazove. Unatoč navedenim komplikacijama, analiza može otkriti širok spektar informacija poput poruka, e-mailova, informacija o pozivima, lokacijskih podataka, multimedijalnih sadržaja te podataka iz različitih aplikacija, [8].

Da bi se ti podaci mogli koristiti na sudu, mora se osigurati da se svi prikupljeni podaci ne kompromitiraju te se mora održavati valjan lanac dokaza. To znači da se moraju pažljivo dokumentirati sve aktivnosti vezane uz uređaj, uključujući prikupljanje, analizu i pohranu podataka. Važno je uzeti u obzir zakonske odredbe o privatnosti prilikom svake faze prikupljanja i korištenja digitalnih dokaza, [7].

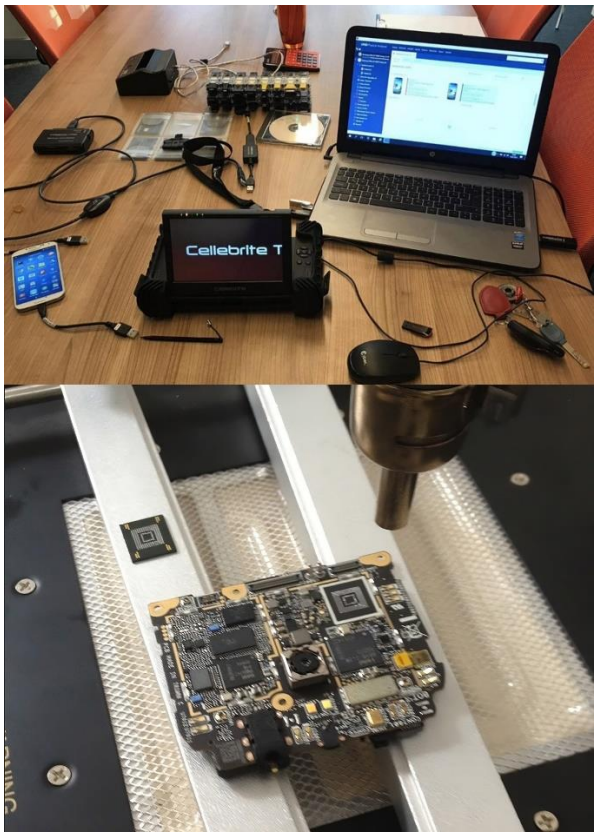
3.2. Metode forenzičke analize pametnih telefona

Forenzička analiza pametnih telefona uključuje različite metode pristupa podacima uređaja. Dok su neki podaci direktno dostupni, drugi su zaštićeni ili izbrisani. Odabrana metoda treba osigurati očuvanje i valjanost dokaza u pravnom kontekstu. Također, pravilan odabir metode ekstrakcije ključan je i ovisi o specifičnostima slučaja i uređaja.

Metode forenzičke analize pametnih telefona obuhvaćaju:

- **Fizička ekstrakcija,** ova metoda pruža pristup sirovim binarnim podacima na uređaju, omogućujući analizu aktivnih, izbrisanih i obično nedostupnih podataka. Nakon ekstrakcije, podaci se analiziraju pomoću forenzičkog softvera, [8].
- **Logička ekstrakcija,** pruža pristup samo aktivnim podacima na uređaju, slično korisničkom sučelju uređaja, [8].
- **Izrada sigurnosne kopije datotečnog sustava,** (engl. *File System Dump*, FSD) metoda je kombinacija fizičke i logičke ekstrakcije, pri čemu se datotečni sustav uređaja ekstrahira i analizira u kasnijim fazama, [8].

- **Ručna metoda,** kada forenzički softver ne podržava određene modele uređaja, može se primijeniti ručna metoda. Ova metoda uključuje zapisivanje prikazanih podataka fotografijama, videom ili ručnim unosom. Preciznost i integritet podataka su kritični, [8].
- **JTAG / Chip-Off / Rooting,** za uređaje s ograničenim pristupom ili oštećene, koriste se JTAG i Chip-Off tehnike. Dok JTAG zahtijeva tehničke intervencije na matičnoj ploči uređaja, Chip-Off uključuje uklanjanje memorijskog čipa s trajnim oštećenjem uređaja. "Rooting" metoda, iako korisna, nije striktno forenzička i može dovesti do promjena ili oštećenja uređaja, [8].



Slika 3. Metode ekstrakcije podataka s mobilnog uređaja, [9], [10]

3.3. Analiza kategorija digitalnih tragova na Android uređajima

Analiza digitalnih tragova na Android uređajima ključan je postupak u digitalnoj forenzici, često otkrivajući vrijedne informacije koje se inače ne bi mogle dobiti. Digitalni tragovi su ostaci informacija koje korisnik ostavlja za sobom prilikom interakcije s uređajem - od web pretraživanja, preko komunikacije putem aplikacija do manipulacije datotekama. S obzirom na sve veću prisutnost Android uređaja, kao i sve veći broj aplikacija i usluga koje korisnici koriste, količina i raznolikost dostupnih digitalnih tragova stalno se povećava.

Svaka kategorija digitalnih tragova pruža jedinstveni uvid u korisničko ponašanje i aktivnosti. Na primjer, informacije o pozivima i porukama mogu otkriti s kim je korisnik komunicirao i kakva je bila priroda te komunikacije, dok podaci o lokaciji mogu otkriti korisnikovu geografsku aktivnost. S druge strane, podaci aplikacija mogu otkriti koje su aplikacije korisnik instalirao i koristio, što može ukazati na korisnikove interese, navike ili rutine uzimajući u obzir etička i privatna pitanja, [7].

Kroz proces forenzičke analize, ovi tragovi se mogu izolirati, analizirati i koristiti za izgradnju detaljne slike o korisnikovom ponašanju, kako je prikazano slikom 4. Ovo znanje može biti od ključne važnosti za rješavanje kriminalnih slučajeva, zaštitu korporativne sigurnosti ili osiguranje privatnosti korisnika.

Kategorije izvora digitalnih tragova obuhvaćaju:

- **Povijest poziva,** sadrži identifikacijske informacije i pruža popis brojeva s kojima je korisnik komunicirao, što može ukazivati na druge relevantne osobe za istragu. Ključni metapodaci poput vremenskih oznaka, koje bilježe početak i kraj svakog poziva, pomažu u rekonstrukciji kronološkog slijeda događaja, dok trajanje poziva može signalizirati prirodu interakcije. Učestalost i vrsta poziva (dolazni, odlazni ili propušteni) pružaju kontekstualne informacije o korisničkim interakcijama. U kombinaciji s drugim digitalnim tragovima, povijest poziva omogućava duboko razumijevanje korisnikovih aktivnosti i komunikacijskih obrazaca, [8].
- **Popis kontakata,** mobilnom uređaju pruža više od imena i brojeva telefona. Forenzičkom analitičaru može služiti kao digitalni resurs za istraživanje korisnikovih veza, bilo osobnih ili profesionalnih. Informacije unutar kontakta mogu obuhvatiti osnovne detalje poput imena i brojeva telefona, ali i proširene informacije poput e-adresa, stvarnih adresa, datuma rođenja i slika. Te informacije olakšavaju identifikaciju osoba povezanih s korisnikom te nude uvide u karakter njihovih odnosa, [8].
- **Email i SMS poruke,** predstavljaju centralne metode komunikacije u suvremenom društvu, nudeći bogat kontekstualni uvid u sadržaj, učestalost i vremenski okvir komunikacije. Emailovi mogu obuhvaćati tekst poruke, adrese pošiljatelja i primatelja, vremenske oznake, naslove, privitke i ponekad informacije o lokaciji. E-mail klijenti omogućuju organizaciju poruka, što može ukazati na način na koji korisnik kategorizira svoje komunikacije. S druge strane, SMS poruke, iako sažetije, pružaju trenutačne informacije o komunikaciji, uključujući telefonske brojeve, vremenske oznake i tekst poruke. Unatoč svom sažetom obliku, SMS poruke mogu biti jednako informativne kao i emailovi tijekom forenzičkih analiza, [8].
- **Medijske datoteke (slike, video, audio),** ključni su izvor informacija o korisničkim aktivnostima, lokacijama i interesima. Slike i videozapisi ne samo da dokumentiraju lokacije, osobe i događaje, već često sadrže metapodatke poput vremenskih oznaka, modela uređaja i GPS koordinata, pružajući dodatni kontekstualni uvid. Dok

audiozapisi, poput snimaka razgovora ili glasovnih bilješki, iako možda ne pružaju vizualni kontekst, mogu biti ključni za razumijevanje korisnikovih interesa i ponašanja u određenim istraživačkim situacijama, [8].

- **Povijest pregleda interneta i pretraživanje ključnih riječi,** pruža uvide o korisnikovim interesima, ponašanju i afilijacijama. Ona otkriva posjećene web stranice, vremenske oznake posjeta i učestalost posjeta. IP adrese i drugi metapodaci mogu dodatno obogatiti ovaj uvid. Međutim, određene korisničke postavke, poput "privatnog" pregleda ili upotrebe VPN-a i Tor preglednika, mogu ograničiti dostupnost ovih podataka, [8].

- **Zapisi iz razgovora i aplikacija za dopisivanje,** danas se široko koriste aplikacije za dopisivanje poput WhatsAppa, Messengera, Vibera, Signala i Telegrama u komunikaciji. Svaka od tih aplikacija koristi specifične metode pohrane i šifriranja informacija. Primjerice, aplikacije kao što je Signal koriste napredne metode šifriranja i ne čuvaju podatke na centraliziranim poslužiteljima, što može postaviti izazove prilikom pokušaja pristupa i analize tih podataka u forenzičkom kontekstu, [8].

- **Korisnički računi na društvenim mrežama,** u suvremenom digitalnom okruženju, društveni mediji nude bogat izvor podataka o korisnikovim interakcijama, interesima i aktivnostima. Platforme kao što su Facebook, Twitter, Instagram, LinkedIn i Snapchat pohranjuju različite vrste informacija, uključujući objave, slike, video sadržaje, interakcije, informacije o lokaciji i detalje profila. No, pristup tim podacima može biti izazovan zbog šifriranja, sigurnosnih mjera i pravila o zaštiti privatnosti koje platforme implementiraju. Uz to, pravni okviri mogu dalje ograničiti dostupnost ovih informacija u forenzičkom kontekstu, [8].

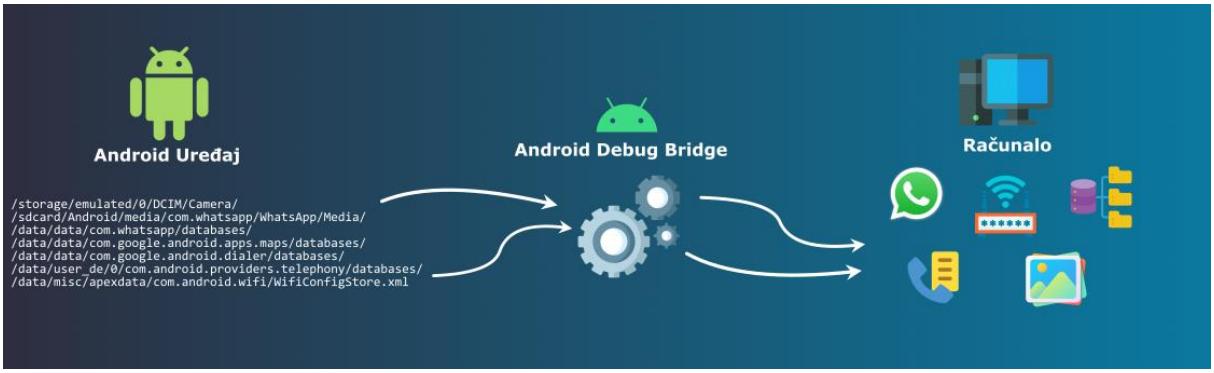
- **Kalendar i bilješke,** podaci korišteni u kalendarima i aplikacijama za bilješke na Android uređajima pružaju informacije o korisnikovim aktivnostima i interesima. Analiza kalendara može otkrivati informacije o sastancima, događajima te vremenskim i lokacijskim oznakama, čime se omogućuje rekonstrukcija korisnikovih aktivnosti. Slično tome, bilješke mogu sadržavati detalje o korisnikovim namjerama i planovima, [8].

- **Mrežne veze (Mobilna mreža, Wi-Fi, Bluetooth),** podaci mobilne mreže, uključujući logove poziva i korištene SIM kartice, pružaju uvide o korisnikovoj telekomunikacijskoj aktivnosti i kretanju. Povezivanje na Wi-Fi mreže indicira specifične lokacije i može pomoći u rekonstrukciji korisnikove rutine. Bluetooth veze otkrivaju interakcije s bliskim uređajima, poput slušalica ili automobila. Kada se kombiniraju, ovi podaci pružaju kontekst za interpretaciju drugih digitalnih tragova, [8].

- **Karte (lokacije, pohranjene rute, favoriti),** kartografski podaci na Android uređajima omogućuju analizu korisnikove geografske aktivnosti kroz povijest GPS lokacija, pohranjenih ruta i omiljenih mjesta. GPS podaci mogu rekonstruirati korisnikove putanje, frekvenciju posjeta određenim lokacijama i brzinu kretanja. Pohranjene rute

u navigacijskim aplikacijama otkrivaju korisnikove namjere ili prethodna putovanja, dok omiljena mjesta pružaju kontekst o korisnikovim navikama. Pristup ovim podacima može biti ograničen postavkama privatnosti i aplikacijama, ali kada su dostupni, pružaju dragocjeni uvid u forenzičku analizu, [8].

- **Softver (Obrada dokumenata, PDF, itd.),** aplikacije za obradu dokumenata i PDF preglednike sadrže podatke o korisničkim aktivnostima, uključujući povijest uređivanja, otvaranja dokumenata i datume kreiranja. Informacije iz ovih aplikacija mogu otkriti korisnikove radne zadatke, projekte i potencijalno osjetljive informacije. PDF preglednici često zadržavaju popis otvorenih dokumenata i mogu sadržavati bilješke korisnika. Međutim, dostupnost ovih podataka može varirati ovisno o postavkama aplikacija i uređaja, iako forenzička analiza može omogućiti povrat nekih informacija, [8].



Slika 4. Razne kategorije podataka ekstrahirane s uređaja

3.4. Procesi i opći zahtjevi

Digitalni dokazi predstavljaju ključnu komponentu suvremenog pravnog sustava, posebice u slučajevima koji uključuju kibernetički kriminal ili druge oblike digitalnih prekršaja. S obzirom na njihovu važnost, izuzetno je bitno da digitalni dokazi budu precizni i točni kako bi se prihvatili na sudu, [7].

Točnost digitalnih dokaza odnosi se na njihovu pouzdanost u odnosu na originalne informacije s uređaja s kojeg su prikupljeni. Svaki dokaz mora biti reprezentacija stvarnih podataka, bez ikakvih izmjena ili manipulacija. To osigurava da se svi dokazi prikupljeni tijekom forenzičke analize mogu smatrati vjerodostojnim i točnim prikazom originalnih podataka, [7].

S druge strane, krhkost digitalnih dokaza odnosi se na njihovu osjetljivost na nepravilno rukovanje ili tehničke pogreške koje mogu dovesti do gubitka ili oštećenja podataka. S obzirom na ovu krhkost, iznimno je važno da se s digitalnim dokazima postupa s najvećom pažnjom i stručnošću. To uključuje primjenu ispravnih metoda ekstrakcije i analize, pridržavanje strogih

protokola za rukovanje dokazima, te očuvanje i dokumentiranje svakog koraka procesa kako bi se osigurala njegova reproduktivnost i integritet, [7].

Upravljanje digitalnim dokazima zahtijeva visoku razinu stručnosti i poznavanja, ali kada se provede pravilno, može pružiti neophodne informacije za sudski postupak i pridonijeti pravednom i učinkovitom pravosuđu, [7].

3.4.1. Održavanje nepristranosti u forenzičkoj analizi

U forenzici Android uređaja ključna je nepristranost, što zahtijeva objektivan pristup tijekom cijelog procesa forenzičke analize, od prikupljanja do tumačenja dokaza. Analitičari trebaju slijediti etičke smjernice, koristiti standardizirane metode, redovito provjeravati svoje zaključke i održavati transparentnost u dokumentaciji. Identifikacija potencijalnih rizika nepristranosti, bilo da su povezani s internim procedurama, vanjskim odnosima ili interakcijama unutar osoblja, treba biti kontinuirana. Međutim, ne sve percepcije odnosa ili aktivnosti nužno predstavljaju stvarni rizik za nepristranost, [7].

3.4.2. Značaj očuvanja povjerljivosti informacija

Forenzički analitičari imaju pristup osjetljivim podacima, stoga je neophodno uspostaviti stroge postupke i politike za zaštitu povjerljivosti. To uključuje ograničenje pristupa, šifriranje, sigurnu pohranu i prijenos te brisanje podataka kada više nisu potrebni. Svi zaposlenici forenzičkog laboratorija moraju biti educirani o važnosti povjerljivosti i pridržavati se relevantnih smjernica. Povjerljivost se mora očuvati tijekom cijelog forenzičkog procesa, osiguravajući da se informacije otkrivaju samo kada je to nužno, a pritom štititi prava pojedinaca i integritet procesa, [7].

3.4.3. Važnost provjerljivosti rezultata u forenzičkim nalazima

Provjerljivost u digitalnoj forenzici zahtijeva detaljne zapise o svim fazama istraživanja. Svaki korak, od prikupljanja do interpretacije podataka, treba biti dokumentiran tako da drugi stručnjak s odgovarajućim znanjem može ponoviti postupak i potvrditi rezultate. Analitičari bi trebali koristiti alate i metode koje su priznate kao pouzdane u stručnoj zajednici, uključujući alate za digitalnu forenziku koji su prošli odgovarajuće testiranje i validaciju, [7].

3.4.4. Ponovljivost postupaka u forenzičkim ispitivanjima

Ponovljivost u kontekstu forenzičke analize odnosi se na sposobnost ponavljanja istog postupka pod jednakim uvjetima te postizanja konzistentnih rezultata. Ova karakteristika je ključna iz više razloga:

1. Robusnost i pouzdanost: Ponovljivost osigurava da su rezultati forenzičke analize stabilni i vjerodostojni. Konzistentni rezultati pri ponovnom testiranju povećavaju povjerenje u nalaze.
2. Neovisna provjera: Omogućuje drugima da provjere valjanost analize. Ako neovisni stručnjaci mogu replicirati postupak i postići iste zaključke, to potvrđuje točnost originalne analize.
3. Pravna prihvatljivost: U pravnom kontekstu, dokazi moraju biti pouzdani. Ako postupci forenzičke analize nisu ponovljivi, može se osporiti njihova valjanost, što može rezultirati odbacivanjem takvih dokaza na sudu, [8].

3.4.5. Reproducibilnost rezultata u forenzičkoj praksi

Dok se ponovljivost odnosi na mogućnost ponavljanja istih rezultata unutar istog okruženja s istim alatima, reproducibilnost podrazumijeva sposobnost dobivanja konzistentnih rezultata koristeći različite alate ili metode, ili čak u različitim okruženjima. U idealnom slučaju, različiti forenzički stručnjaci trebali bi moći doći do istih zaključaka koristeći različite metode, [7].

Reproducibilnost je od ključne važnosti za utvrđivanje pouzdanosti i objektivnosti digitalne forenzičke analize. To omogućava neovisnim stranama da potvrde nalaze izvornog analitičara, čak i ako koriste drugačije alate ili metode. Također, to pomaže u otkrivanju mogućih pogrešaka, pristranosti ili netočnosti u izvornoj analizi, [7].

3.4.6. Kriteriji opravdanosti zaključaka u forenzičkoj analizi

Opravdanost je neophodna kako bi rezultati analize bili prihvaćeni kao valjani i relevantni, bilo u sudskom procesu ili drugim kontekstima. Digitalni forenzičari moraju biti sposobni opravdati sve korake koje su poduzeli tijekom analize, uključujući odabir korištenih alata i tehnika, interpretaciju rezultata i zaključke koje su donijeli na temelju tih rezultata. Svi koraci moraju biti temeljeni na čvrstoj znanstvenoj osnovi i moraju biti usklađeni s etičkim smjernicama i pravilima struke, [7].

3.4.7. Održavanje integriteta kroz lanac nadzora

Lanac nadzora predstavlja ključnu komponentu digitalne forenzičke istrage, odražavajući kontinuirani zapis svih interakcija s digitalnim dokazima od trenutka njihove identifikacije do prezentacije na sudu, [7].

Ova dokumentacija obuhvaća svaku akciju vezanu uz dokaze, uključujući datum, vrijeme, identitet osobe koja je intervenirala i prirodu te intervencije. Ovaj pristup osigurava autentičnost i cjelovitost dokaza, potvrđujući da nisu kompromitirani ili neovlašteno mijenjani. Sveukupna prihvatljivost dokaza na sudu ovisi o neprekinutom lancu nadzora. Prekidi u ovom lancu mogu dovesti do pitanja o vjerodostojnosti dokaza. Da bi se uspješno održao lanac nadzora, neophodne su čvrste procedure, edukacija osoblja i ispravna primjena forenzičkih metoda, uz strogo pridržavanje pravila vezanih za rukovanje digitalnim dokazima, [7].

4. Alati za forenzičku analizu Android uređaja

Forenzička analiza digitalnih uređaja postala je ključni dio modernih istraživačkih postupaka. S obzirom na sveprisutnost mobilnih uređaja, posebno onih koji koriste Android operativni sustav, potreba za preciznim i pouzdanim alatima za njihovu analizu nikada nije bila veća. Ovi alati omogućuju stručnjacima da izvlače podatke, proučavaju ih te rekonstruiraju događaje, često otkrivajući ključne informacije koje mogu biti presudne u istražnim postupcima.

Dok Android uređaji imaju svoje specifičnosti, osnovna načela digitalne forenzike ostaju konzistentna kroz različite platforme i uređaje. Međutim, uspoređujući alate za Android s onima namijenjenima drugim operativnim sustavima, poput Windowsa ili macOS-a, primjećujemo nekoliko ključnih razlika. Android, kao otvoreni sustav baziran na Linuxu, ima jedinstvenu strukturu i sigurnosne mehanizme. Stoga, alati dizajnirani za Android moraju biti prilagođeni kako bi se suočili s ovim jedinstvenim izazovima. Dok neki alati mogu pružiti širok spektar funkcionalnosti preko raznih platformi, specifični alati za Android često nude dublje i preciznije mogućnosti za analizu upravo na ovoj platformi.

4.1. Kriteriji odabira alata

Pri odabiru alata za forenzičku analizu Android uređaja, bitno je razmotriti niz kriterija kako bi se osiguralo da alat odgovara specifičnim potrebama i okolnostima analize. Sljedeći kriteriji trebaju biti u središtu svake odluke, [7]:

1. **Pouzdanost i točnost**: Forenzički alati moraju pružiti dosljedne i točne rezultate. Svaka greška ili nepouzdanost u ekstrakciji ili analizi podataka može dovesti do pogrešnih zaključaka ili čak ugroziti pravnu valjanost dokaza. Pouzdanost također znači da alat konzistentno radi bez padova ili drugih problema.
2. **Kompatibilnost s različitim verzijama Androida**: Android operativni sustav je poznat po svojoj fragmentiranosti. Uz različite verzije sustava koje su aktivno u upotrebi, postoji i mnoštvo proizvođača koji prilagođavaju Android za svoje uređaje. Idealni alat trebao bi podržavati širok spektar verzija i prilagodbi, osiguravajući time fleksibilnost u različitim situacijama.
3. **Sposobnost izvlačenja zaštićenih ili izbrisanih podataka**: Često su najvažniji podaci oni koji su bili izbrisani ili su zaštićeni raznim mehanizmima. Alat mora imati mogućnost penetracije kroz sigurnosne slojeve te rekonstrukcije izbrisanih podataka.
4. **Intuitivnost sučelja i lakoća korištenja**: Dok je tehnička sofisticiranost alata ključna, također je bitno da je sučelje intuitivno i lako za korištenje. To omogućuje brži i efikasniji rad, smanjujući mogućnost grešaka i omogućavajući analitičarima da se usredotoče na analizu, a ne na borbu s kompleksnim sučeljem.

Osim navedenih, postoji niz drugih specifičnih kriterija koji mogu biti relevantni ovisno o specifičnoj situaciji i potrebama analize, ali ovi predstavljaju osnovu koja bi trebala biti uzeta u obzir prilikom svakog odabira.

4.2. Pregled trenutno dostupnih alata

S obzirom na sve veći broj digitalnih uređaja i informacija koje oni sadrže, potreba za sofisticiranim alatima koji mogu efikasno ekstrahirati i analizirati te podatke nikada nije bila veća. Dok besplatni alati nude temeljne mogućnosti, komercijalne solucije često pružaju širi spektar funkcionalnosti, dodatne resurse i podršku, što ih čini izborom mnogih profesionalnih analitičara.

4.2.1. Cellebrite UFED

Cellebrite UFED (engl. *Universal Forensic Extraction Device*) je jedno od vodećih rješenja na tržištu kada je riječ o ekstrakciji i analizi podataka s mobilnih uređaja. Ovaj alat je posebno dizajniran za dubinsku ekstrakciju podataka, uključujući one koji su zaštićeni ili izbrisani. UFED može pristupiti podacima s raznih uređaja, uključujući pametne telefone, tablete, memorijske kartice i druge digitalne uređaje, [11].

Njegove značajke uključuju, ali nisu ograničene na, vizualni pregled podataka, pretragu ključnih riječi, izradu vremenskih crta aktivnosti i mnoge druge. S obzirom na širok spektar podrške i kontinuirane nadogradnje, Cellebrite UFED je čest izbor među organima provođenja zakona, vojnim organizacijama i forenzičkim analitičarima širom svijeta, [11].

4.2.2. Oxygen Forensics

Oxygen Forensics je još jedno sveobuhvatno rješenje namijenjeno forenzičkoj analizi digitalnih uređaja. Dok je ovaj alat također sposoban ekstrahirati podatke s raznih uređaja, on pruža dodatne mogućnosti analize i obrade tih podataka, često koristeći grafičke prikaze i vizualizacije za bolju interpretaciju informacija, [12].

Jedna od ključnih prednosti Oxygen Forensics je njegova integracija s različitim bazama podataka i cloud uslugama, što analitičarima omogućuje da pristupe informacijama koje nisu nužno fizički pohranjene na uređaju. Osim toga, njegove analitičke mogućnosti omogućuju korisnicima da pravilno interpretiraju složene podatke, kao što su podaci o lokaciji, komunikacije putem društvenih mreža i drugo. Kao i UFED, Oxygen Forensics je izbor mnogih profesionalaca zahvaljujući svojoj sveobuhvatnosti i pouzdanosti, [12].

4.3. Besplatni i otvoreni alati

Dok neki od ovih alata dolaze s visokom cijenom i sofisticiranim funkcionalnostima, postoji i značajan broj besplatnih i otvorenih alata koji pružaju kvalitetnu funkcionalnost bez dodatnih troškova. Ovi alati često postaju omiljeni među forenzičarima zbog svoje transparentnosti, zajedničkog doprinosa zajednice i mogućnosti prilagodbe.

4.3.1. Alat Android Debug Bridge

ADB, ili Android Debug Bridge, predstavlja svestran alat koji omogućava komunikaciju između računala i Android uređaja. Omogućava korisnicima da izvršavaju različite naredbe na uređaju iz terminala svog računala, pružajući duboki pristup funkcionalnostima i podacima uređaja, [13].

Zbog svoje sposobnosti pružanja direktne komunikacije s uređajem, ADB je postao neophodan alat u forenzičkoj analizi Android uređaja. Omogućava forenzičarima izravan pristup uređaju, izvlačenje značajnih podataka, provjeru stanja sustava i, u nekim slučajevima, čak i povrat izbrisanih informacija. Osim što je moćan, ADB je i fleksibilan. Njegove funkcionalnosti mogu se proširiti pomoću skripti i dodatnih alata.

S obzirom na njegovu snažnu i prilagodljivu prirodu, ADB će i dalje ostati temeljni alat u arsenalu svakog forenzičkog analitičara koji se bavi analizom Android uređaja.

4.3.2. Alat Autopsy

Autopsy je sveobuhvatan digitalno-forenzički platformski alat koji služi za pregled i analizu različitih digitalnih dokaza. Iako se ne koristi isključivo za Android uređaje, njegove bogate funkcionalnosti čine ga izuzetno korisnim za analizu podataka s mobilnih uređaja, [14].

Autopsy nudi grafičko sučelje koje olakšava analizu, pretraživanje, izvještavanje i dokumentaciju digitalnih dokaza. Njegove osnovne značajke uključuju vremenske crte, pretragu ključnih riječi, analizu metapodataka i pregled izbrisanih datoteka. Osim toga, Autopsy podržava širok spektar dodataka, što ga čini prilagodljivim za različite forenzičke zadatke i scenarije, [14].

U kontekstu Androida, Autopsy može pružiti analitičaru pristup raznim segmentima uređaja, kao što su SMS poruke, povijest poziva, fotografije, aplikacijski podaci i mnoge druge.

Kada se koristi u kombinaciji s ADB za ekstrakciju podataka, Autopsy omogućava temeljitiju analizu ekstrahiranih podataka, nudeći široki spektar forenzičkih alata i metoda. Zahvaljujući svojoj aktivnoj zajednici koja doprinosi kontinuiranim nadogradnjama, Autopsy se održava kao jedan od ključnih alata u digitalnoj forenzici, posebno za analizu Android uređaja, [15], [16].

5. Ekstrakcija podataka Android uređaja

Ekstrakcija podataka koristeći Android Debug Bridge (ADB) metodu ilustrira ne samo tehničke vještine potrebne za digitalnu forenziku, već i složenost i detaljnost koja ide uz ovu vrstu analize.

Ovaj dio rada fokusirat će se na praktičnu primjenu ADB metode za ekstrakciju podataka s Android uređaja. Detaljno će biti opisani koraci koji su uključeni u ovaj postupak, počevši od pripreme uređaja za proces ekstrakcije pa sve do primjene specifičnih ADB i Linux naredbi.

5.1. Priprema Android uređaja za ekstrakciju

Priprema Android uređaja ključna je faza u procesu ekstrakcije podataka. U ovom slučaju, koristi se Xiaomi 11i uređaj koji pokreće Android 13. Uređaj ima root pristup. Treba istaknuti da je uređaj zaštićen šifrom, no za potrebe ove analize pretpostavljamo da postoji pristup toj šifri. Prvi korak u pripremi uređaja je omogućavanje USB debugginga. Ova opcija omogućuje uređaju da komunicira s računalom putem Android Debug Bridge (ADB) protokola.

5.1.1. Povezivanje uređaja s računalom

Nakon što je USB debugging omogućen, uređaj se može povezati s računalom koristeći USB kabel. Kada se uređaj prvi put poveže s računalom, na uređaju će se pojaviti prozor koji traži odobrenje za USB debugging. Potrebno je potvrditi i dozvoliti povezivanje.

Slika 5. Zahtjev koji nastaje tijekom uspostavljanja veze s računalom

5.1.2. Provjera povezanosti s ADB-om

Nakon povezivanja uređaja s računalom, potrebno je provjeriti je li uređaj pravilno povezan koristeći ADB. Na računalu, otvori se terminal ili command prompt, a zatim unese sljedeća naredba: `adb devices`. Rezultat bi trebao prikazati popis povezanih uređaja:

```
> adb devices
List of devices attached
2c6ae187        device
```

Prije nego što se pristupi uređaju putem `adb shell-a`, potrebno je inicijalizirati adb u root modu koristeći naredbu `adb root`.

Nakon ovih koraka, uređaj je pripremljen i spreman za daljnju obradu i ekstrakciju podataka.

5.1.3. Adb shell

ADB Shell je važan alat koji omogućuje korisnicima da izvršavaju naredbe na Android uređaju putem računala. Shell je zapravo sučelje koje omogućuje komunikaciju između korisnika i operativnog sustava putem naredbi. ADB Shell pruža mogućnost da se te naredbe izvršavaju na Android uređaju putem računala, što može biti iznimno korisno za različite zadatke, uključujući i forenzičku analizu.

Kako bi se pristupilo ADB Shellu, unosi se naredba: `adb shell`. Ova naredba pokreće shell sesiju za povezani Android uređaj. Nakon toga, moguće je izvršavati različite naredbe direktno na uređaju.

U poglavlju 2.3.2., koje se odnosi na hijerarhiju datoteka na Androidu, pojašnjeno je kako model upravljanja datotekama Androida zapravo reflektira postojeću hijerarhiju Linuxa, operativnog sustava na kojem se Android temelji. Kako bi se olakšala navigacija kroz ovu strukturu i povećala njena korisnost u kontekstu forenzičke analize, u nastavku je detaljno objašnjeno nekoliko ključnih naredbi koje omogućuju efikasno kretanje kroz datotečni sustav, kao i druge koje su korisne za daljnji rad:

- `ls`: Omogućuje prikazivanje sadržaja trenutačne direktorije.

```
haydn:/ # ls
acct          debug_ramdisk    odm                    sys
apex          dev              odm_dlkm               system
bin           etc              oem                    system_dlkm
bugreports    init             postinstall            system_ext
cache         init.environ.rc  proc                   vendor
config        linkerconfig     product                vendor_dlkm
d             lost+found       sdcard
data          metadata         second_stage_resources
```

- `cd [ime direktorija]`: Koristi se za promjenu trenutačne direktorije na onu koja je navedena.

```
haydn:/ # cd data/misc/apexdata
haydn:/data/misc/apexdata #
```

- `pwd`: Prikazuje putanju trenutačne direktorije.

```
haydn:/data/misc/apexdata # pwd
/data/misc/apexdata
```

- `cat`: Koristi se za prikaz sadržaja datoteke.

```
haydn:/ # cat /system/build.prop
#####################################
# from generate-common-build-props
# These properties identify this partition image.
#####################################
ro.product.system.device=haydn
ro.product.system.brand=Xiaomi
ro.product.system.manufacturer=Xiaomi
ro.product.system.model=M2012K11G
ro.product.system.name=haydn_global
.........
```

- `grep`: Koristi se za pretraživanje teksta.

```
haydn:/ # getprop | grep imei
[persist.vendor.radio.imei1]: [8659700548xxxx8]
[persist.vendor.radio.imei2]: [8659700548xxxx6]
```

- `find`: Koristi se za pretraživanje datoteka ili direktorija.

```
haydn:/ # find . -name 'com.android.wifi' -type d
./apex/com.android.wifi
./data/misc/apexdata/com.android.wifi
./data/misc_de/0/apexdata/com.android.wifi
./data/misc_ce/0/apexdata/com.android.wifi
```

5.2. Ekstrakcija podataka pomoću ADB-a

Ekstrakcija podataka s Android uređaja koristeći Android Debug Bridge (ADB) metodu omogućuje pristup i kopiranje velikog broja datoteka i informacija s uređaja. To uključuje sve, od sistemskih datoteka do korisničkih podataka, poput kontakata, poruka, fotografija, videozapisa, datoteka aplikacija i još mnogo toga. Postupak ekstrakcije podataka pomoću ADB-a sastoji se od različitih koraka, koji će biti detaljno objašnjeni u ovom poglavlju.

5.2.1. Ekstrakcija podataka s vanjske pohrane

Vanjska pohrana na Android uređaju obično se koristi za pohranu većine korisničkih podataka, kao što su fotografije, videozapisi, glazba i datoteke preuzete s Interneta. Vanjska pohrana također može sadržavati podatke aplikacija koje su korisniku instalirane na uređaju.

```
haydn:/storage/emulated/0 # ls -l
total 53torage/emulated/0 #
```

```
drwxrws---  2 u0_a162  media_rw 3452 2023-05-22 17:16 Alarms
drwxrws--x  5 media_rw media_rw 3452 2023-05-22 17:16 Android
drwxrws---  2 u0_a162  media_rw 3452 2023-05-22 17:16 Audiobooks
drwxrws---  6 u0_a162  media_rw 3452 2023-06-30 10:35 DCIM
drwxrws---  2 u0_a162  media_rw 3452 2023-05-22 17:16 Documents
drwxrws---  7 u0_a162  media_rw 8192 2023-07-12 12:32 Download
drwxrws---  5 u0_a162  media_rw 3452 2023-07-04 00:34 LMC8.4
drwxrws---  4 u0_a162  media_rw 3452 2023-06-29 19:23 Movies
drwxrws---  4 u0_a162  media_rw 3452 2023-06-28 23:37 Music
drwxrws---  2 u0_a162  media_rw 3452 2023-06-26 12:04 Notifications
drwxrws--- 11 u0_a162  media_rw 3452 2023-08-01 22:17 Pictures
drwxrws---  2 u0_a162  media_rw 3452 2023-05-22 17:16 Podcasts
drwxrws---  2 u0_a162  media_rw 3452 2023-05-22 17:16 Recordings
drwxrws---  2 u0_a162  media_rw 3452 2023-05-22 17:16 Ringtones
drwxrws---  2 u0_a162  media_rw 3452 2023-07-03 17:49 WearOS
drwxrws---  2 u0_a162  media_rw 3452 2023-07-31 22:31 boot_a
```

5.2.2. Ekstrakcija podataka s unutarnje pohrane

Unutarnja pohrana uređaja obično sadrži sustav Android, aplikacije i njihove podatke, kao i neke korisničke podatke koji nisu smješteni na vanjskoj pohrani. Pristupanje unutarnjoj pohrani može biti složenije zbog sigurnosnih mjera koje Android implementira za zaštitu podataka korisnika i integriteta sustava.

Podaci koji će najviše koristiti nalaze se u mapi `/data/data`:

```
haydn:/ # ls /data/data
com.adobe.reader
com.aftership.AfterShip
com.airbnb.android
com.alibaba.aliexpresshd
com.amazon.mShop.android.shopping
com.android.adservices.api
com.android.backupconfirm
com.android.bips
com.android.bluetooth
com.android.calllogbackup
..........
```

5.2.3. Ekstrakcija podataka aplikacija

Podaci aplikacija mogu uključivati sve od postavki aplikacije do korisničkih podataka unutar aplikacije. To mogu biti poruke iz aplikacija za razmjenu poruka, zapisi poziva, dokumenti, fotografije, videozapisi i još mnogo toga. Ovi podaci obično su pohranjeni unutar posebnih direktorija unutar unutarnje pohrane uređaja.

Datoteke SQLite baza podataka obično se pohranjuju u unutarnjoj pohrani pod `/data/data/<ime_aplikacijskog_paketa>/databases`. Međutim, nema ograničenja za stvaranje baza podataka negdje drugdje.

U slučajevima primjene prikazanim tablicom ispod ekstrahirani su podaci aplikacija koje potencijalno sadrže korisne informacije:

Aplikacija	Naredba
WhatsApp	`>adb pull /data/data/com.whatsapp/databases F:\ExtractedData /data/data/com.whatsapp/databases/: 39 files pulled, 0 skipped. 38.1 MB/s (131848432 bytes in 3.299s)`
Instagram	`>adb pull /data/data/com.instagram.android/databases F:\ExtractedData /data/data/com.instagram.android/databases/: 52 files pulled, 0 skipped. 30.7 MB/s (17737176 bytes in 0.551s)`
Google Chrome	`>adb pull /data/data/com.android.chrome/app_chrome F:\ExtractedData /data/data/com.android.chrome/app_chrome/: 1263 files pulled, 0 skipped. 6.8 MB/s (28218383 bytes in 3.945s)`
Google Maps	`>adb pull /data/data/com.google.android.apps.maps/databases F:\ExtractedData /data/data/com.google.android.apps.maps/databases 52 files pulled, 0 skipped. 25.2 MB/s (13792424 bytes in 0.522s)`
Kalendar	`>adb pull /data/data/com.android.providers.calendar/databases F:\ExtractedData /data/data/com.android.providers.calendar/databases 2 files pulled, 0 skipped. 6.3 MB/s (167936 bytes in 0.025s)`
SMS poruke	`>adb pull /data/data/com.google.android.apps.messaging /databases F:\ExtractedData /data/data/com.google.android.apps.messaging/databases/: 10 files pulled, 0 skipped. 21.5 MB/s (2235016 bytes in 0.099s)`
Kontakti i pozivi	`>adb pull /data/data/com.google.android.dialer/databases F:\ExtractedData /data/data/com.google.android.dialer/databases/: 33 files pulled, 0 skipped. 12.0 MB/s (2014232 bytes in 0.160s)`

Tablica 1. Ekstrahirani podaci aplikacija

U opisanom slučaju tablica predstavlja ekstrakcije podataka iz određenih aplikacija. Naredba je specifična za Android platformu i koristi se za ekstrakciju podataka. Evo što komanda konkretno radi:

1. `adb pull`: "`pull`" je specifična komanda koja omogućuje kopiranje datoteka s Android uređaja na računalo.
2. `/data/data/<ime_aplikacijskog_paketa>/databases`: putanja na Android uređaju gdje aplikacija pohranjuje svoje baze podataka.
3. `F:\ExtractedData`: odredište na računalu gdje će biti kopirane i pohranjene izvučene datoteke.
4. Nakon izvršenja komande, prikazuje se rezultat: "`39 files pulled, 0 skipped. 38.1 MB/s (131848432 bytes in 3.299s)`". To znači da je 39 datoteka uspješno kopirano s Android uređaja na računalo, nijedna datoteka nije preskočena, brzina prijenosa bila je 38.1 MB/s, a ukupno je preneseno 131,848,432 bajta u 3.299 sekundi.

Uzimajući u obzir ovu komandu, može se zaključiti da je naredba uspješno ekstrahirala baze podataka aplikacije određenog Android uređaja i pohranila ih na svoje računalo na specificiranu lokaciju za daljnju analizu.

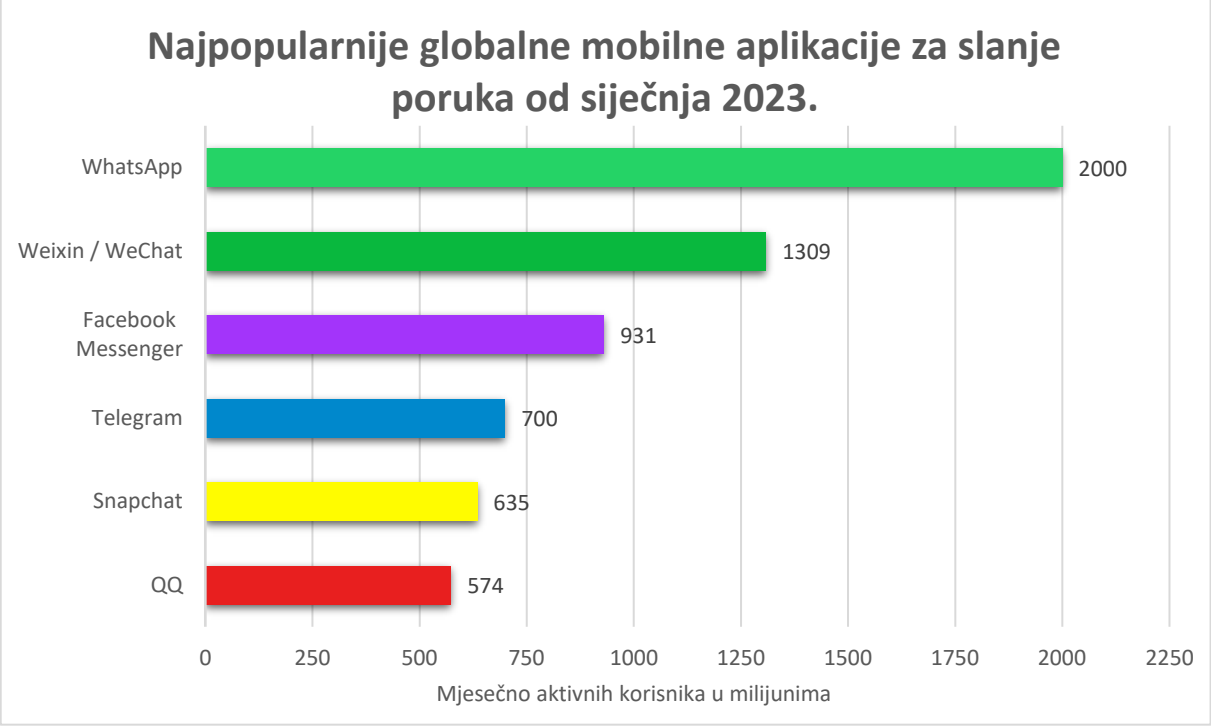
6. Analiza ekstrahiranih podataka i izvještaj

Nakon ekstrakcije podataka s Android uređaja, ključna faza svake forenzičke analize jest interpretacija i analiza tih podataka. Kao centralni alat uz ADB Shell u ovoj fazi koristi se DB Browser for SQLite [17], koji s prilagođenim upitima omogućava sofisticirano i smisleno formatiranje podataka iz baza, čime se osigurava jasnoća i preciznost prilikom njihove interpretacije.

6.1. Analiza podataka ekstrahiranih iz aplikacija

6.1.1. Analiza podataka ekstrahiranih iz aplikacije WhatsApp

WhatsApp je među najčešće korištenim aplikacijama za razmjenu poruka i obavljanje poziva diljem svijeta kao što vidimo u grafu 2. Zbog svoje raširenosti, od izuzetne je važnosti u forenzičkim analizama, jer postoji visoka vjerojatnost da su ključne poruke poslane upravo putem ove aplikacije.



Graf 2. Najpopularnije globalne mobilne aplikacije za slanje poruka
Izvor: [18]

Proučavajući WhatsApp aplikaciju, može se pristupiti bogatom skupu informacija. Datoteka imenovana `msgstore.db` pohranjuje sve poruke, pozive, grupne razgovore, poslane lokacije, putanje do datoteka i slika, glasovne poruke i slične podatke. Zbog složenosti ove baze podataka, SQL upiti bit će podijeljeni u dvije kategorije: prva obuhvaća poruke i sve povezano s njima, dok druga cilja na pozive i video pozive.

Prva tablica koja će biti pretraživana je `message`. Ova tablica čuva sve primljene i poslane poruke. Bez konkretnog uvida u sve informacije razgovora korisnika, tablica pruža osnovnu sliku komunikacije. Stupac `from_me` s vrijednošću `1` označava poruke koje je korisnik poslao, dok vrijednost `0` ukazuje na primljene poruke. `formatedTime` prikazuje vrijeme poruke pretvoreno iz Unix timestampa. Stupac `message_type` razvrstava poruke prema vrsti, a s dostupnim informacijama, vrijednosti su sljedeće:

message_type	Opis
0	Tekstualna poruka
1	Slika
2	Audio zapis ili glasovna poruka
3	Video zapis
4	Dijeljeni kontakti
5	Poruka s lokacijom
9	Dokument
13	Animirani GIF
20	Sticker

Tablica 2. Opis message_type vrijednosti

Tekst poruke pohranjen je u `text_data`. Spajanjem tablica `chat`, `message` i `jid`, dobivaju se detaljniji podaci o sugovornicima, što je vidljivo iz stupca `user` koji prikazuje njihove brojeve. Za poruke koje sadrže geolokacijske informacije, podaci su povezani s tablicom `message_location`, iz koje se izvlače geolokacijske koordinate - `latitude` i `longitude`. Putanja do poslane datoteke na uređaju nalazi se u koloni `file_path`, koja je rezultat spajanja s tablicom `message_media`. Ovu putanju je moguće iskoristiti za izvlačenje datoteke upotrebom `adb pull` naredbe. Stupac `display_name` je povezan s bazom podataka `dialer.db`, koja se nalazi pod `/com.google.android.dialer/databases/`. Spajanjem tablice `smartdial_table` s `jid.user`, prikazuje se samo `display_name`, što predstavlja ime kontakta kako je spremljeno u kontaktima uređaja.

SQL upit i slike ispisa podataka prikazani su ispod:

```
SELECT message._id AS 'message._id'
       ,chat._id AS 'chat._id'
       ,jid._id AS 'jid._id'
       ,message.from_me
       ,DATETIME(message.timestamp/1000,'unixepoch') AS 'formatedTime'
       ,message.message_type
       ,message.text_data
       ,jid.user
       ,message_location.latitude
       ,message_location.longitude
       ,message_media.file_path
       ,contactsdb.display_name
FROM message
INNER JOIN chat
  ON chat._id=message.chat_row_id
```

```
INNER JOIN jid
  ON jid._id=chat.jid_row_id
LEFT JOIN message_location
  ON message_location.message_row_id=message._id
LEFT JOIN message_media
  ON message_media.message_row_id=message._id
LEFT JOIN dialer.smartdial_table AS 'contactsdb'
  ON contactsdb.normalized_number=jid.user
GROUP BY message._id
```

	message._id	chat._id	jid._id	from_me	formatedTime	message_type	text_data	user	latitude	longitude	file_path	display_name
66	81122	24	41	0	2019-11- 10:04:50	1	NULL	38599	NULL	NULL	Media/WhatsApp Images/IMG-	Andrija
67	82521	24	41	0	2019-11- 07:13:12	9		38599	NULL	NULL	Media/WhatsApp Documents/...	Andrija
68	82679	24	41	0	2019-11- 21:11:03	9		38599	NULL	NULL	Media/WhatsApp Documents/	Andrija
69	84123	24	41	1	2019-11- 13:35:32	1	Jeste vi koristili ovaj predložak za prezentaciju ili ...	38599	NULL	NULL	Media/WhatsApp Images/Sent/	Andrija
70	84125	24	41	0	2019-11- 13:38:22	1	NULL	38599	NULL	NULL	Media/WhatsApp Images/IMG-	Andrija
71	84126	24	41	0	2019-11- 13:38:22	1	NULL	38599	NULL	NULL	Media/WhatsApp Images/IMG-	Andrija
72	85097	24	41	1	2019-11- 10:53:49	1		38599	NULL	NULL	Media/WhatsApp Images/Sent/	Andrija
73	85109	24	41	1	2019-11- 12:13:39	1		38599	NULL	NULL	Media/WhatsApp Images/Sent/	Andrija
74	94708	24	41	1	2020-01- 18:44:50	1		38599	NULL	NULL	Media/WhatsApp Images/Sent/	Andrija
75	94714	24	41	1	2020-01- 18:50:18	1		38599	NULL	NULL	Media/WhatsApp Images/Sent/	Andrija
76	96182	24	41	1	2020-01- 19:29:21	1		38599	NULL	NULL	Media/WhatsApp Images/Sent/	Andrija
77	97615	24	41	1	2020-01- 18:08:22	9		38599	NULL	NULL	Media/WhatsApp Documents/	Andrija
78	102780	24	41	1	2020-02- 19:07:55	1		38599	NULL	NULL	Media/WhatsApp Images/Sent/	Andrija

Slika 6. msgstore.db s filterom: `HAVING display_name='Andrija' AND file_path IS NOT NULL`

	message._id	chat._id	jid._id	from_me	formatedTime	message_type	text_data	user	latitude	longitude	file_path	display_name
1	75262	3	17	1	2019-10- 10:50:11	5	NULL	385958	45.8	15.9	NULL	
2	128447	17	35	1	2020-07- 06:42:19	5	NULL	385998	45.7	16.0	NULL	Ivan
3	248330	65	176	0	2022-05- 08:36:21	5	NULL	385989	45.6	15.9	NULL	Eugen
4	257640	8	12	1	2022-10- 19:00:49	5	NULL	385955	45.7	15.9	NULL	Ivona
5	258271	92	937	0	2022-10- 18:11:03	5	NULL	385919	44.4	15.6	NULL	Hrvoje

Slika 7. msgstore.db s filterom: `HAVING message.message_type='5'`

Sljedeća tablica na kojoj će se fokusirati je `call_log`. Ova tablica arhivira sve zapise o pozivima, bilo da je riječ o standardnim glasovnim ili video pozivima. Stupac `from_me` funkcionira isto kao u prethodnoj tablici: vrijednost `1` ukazuje na pozive koje je korisnik inicirao, dok `0` označava primljene pozive. `formatedTime` predstavlja pretvoreno vrijeme poziva iz Unix timestampa. Ako stupac `video_call` sadrži vrijednost `1`, to ukazuje da je riječ o video pozivu. Stupac `callDuration` prikazuje vrijeme trajanja svakog pojedinačnog poziva. Za identifikaciju broja s kojim korisnik komunicira, informacije se povezuju s tablicom `jid`, gdje se brojevi traže u stupcu `user`. Kao i u prethodnom slučaju, `display_name` se dobiva integracijom s bazom podataka `dialer.db`.

SQL upit i slike ispisa podataka prikazani su ispod:

```
SELECT  call_log._id
       ,call_log.jid_row_id
       ,call_log.from_me
       ,DATETIME(call_log.timestamp/1000,'unixepoch') AS 'formatedTime'
       ,call_log.video_call
       ,TIME(call_log.duration,'unixepoch') AS 'callDuration'
       ,jid.user
       ,contactsdb.display_name
FROM call_log
INNER JOIN jid
  ON jid._id = call_log.jid_row_id
LEFT JOIN dialer.smartdial_table AS 'contactsdb'
  ON contactsdb.normalized_number=jid.user
GROUP BY call_log._id
```

	_id	jid_row_id	from_me	formatedTimestamp	video_call	callDuration	user	display_name
79	246	29	0	2020-09- 17: :00	0	00:03:39	385996	
80	249	29	0	2020-09- 17: :55	1	00:20:17	385996	
81	250	29	0	2020-09- 16: :10	0	00:01:16	385996	
82	254	29	1	2020-09- 09: :08	0	00:05:07	385996	
83	255	36	0	2020-09- 10: :24	0	00:00:35	385993	Ivona
84	256	36	1	2020-09- 10: :32	0	00:00:21	385993	Ivona
85	262	22	1	2020-10- 17: :29	0	00:00:22	385994	
86	271	12	0	2020-11- 11: :35	0	00:00:06	385955	
87	284	29	1	2020-12- 16: :46	0	00:00:18	385996	
88	289	29	1	2020-12- 11: :04	0	00:01:36	385996	
89	307	12	0	2021-04- 17: :10	1	00:00:46	385955	
90	308	12	0	2021-04- 08: :09	1	00:00:53	385955	

Slika 8. msgstore.db s filterom `HAVING callDuration!='00:00:00'`

6.1.2. Analiza podataka ekstrahiranih iz aplikacije Instagram

Analizirajući bazu podataka `direct.db` povezanu s Instagram aplikacijom, omogućen je pristup svim poslanim i primljenim porukama na uređaju.

Glavna tablica koja arhivira sve inicirane razgovore jest `threads`. Unutar ove tablice, stupac `recipient_ids` prikazuje ID korisnika s kojim je započet razgovor. Budući da se ovdje prikazuje samo korisnički ID, postupak identifikacije stvarnog imena korisnika zahtijeva dodatne korake. Jedan od metoda je korištenje web stranice za dekodiranje korisničkog ID-a u username, [19]. Nakon unosa ID-a na navedenu web stranicu, prikazuje se korisničko ime povezano s tim ID-em.

_id	user_id	thread_id	recipient_ids	last_activity_time	is_permitted	thread_info
14336	394656	340282366841710300949128170348137 803	214048	2023-07- 20:27:55	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14337	394656	340282366841710300949128429833505 277	483121	2023-06- 20:05:07	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14338	394656	340282366841710300949128133534671 798	470097	2023-06- 17:26:09	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14339	394656	340282366841710300949128117536043 600	144125	2023-04- 14:13:55	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14340	394656	340282366841710300949128115238649 944	228489	2023-04- 14:23:00	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14341	394656	340282366841710300949128139304870 336	229659	2023-04- 22:18:40	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14342	394656	340282366841710301244258961245053 976	262219	2023-04- 20:35:14	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14343	394656	340282366841710300949128130748036 372	552045	2023-02- 22:25:50	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14344	394656	340282366841710300949128236876311 607	402963	2022-11- 20:43:21	1	{"life_cycle_state":"UPLOADED","last_seen_at":...
14375	394656	340282366841710300949128131066370 878	161104	2023-08- 16:53:20	1	{"life_cycle_state":"UPLOADED","last_seen_at":...

Slika 9. Ispis Instagram razgovora

Alternativna metoda uključuje pregled stupca `thread_info`, koji sadrži JSON formatirane podatke. Unutar ovog zapisa može se pretraživati ključna riječ `thread_title`. Ovaj podatak otkriva puno ime i prezime korisnika, pod uvjetom da je korisnik naveo te informacije unutar Instagramove sekcije "Name". Također, ključna riječ `profile_pic_url` vodi do linka koji prikazuje profilnu sliku dotičnog korisnika.

Prilikom dublje analize poruka unutar Instagramove baze podataka, stupac `message` služi kao ključna referenca. Ovaj stupac sadrži podatke u JSON formatu, koji pruža obilje informacija

vezanih za sadržaj i tip poruke. Različite vrste poruka i njihovi odgovarajući podaci mogu se identificirati kako slijedi:

- TEXT - Odnosi se na obične tekstualne poruke. Sadržaj poruke možemo pronaći unutar stupca `text`
- MEDIA - Ova kategorija predstavlja slike poslane s uređaja pošiljatelja. Ako se pretraži JSON stupac messages, može se doći i do mjesta na serveru gdje je pohranjena slika. `("media": > "image_versions2": > "candidates": > "url":)`
- XMA_MEDIA_SHARE - Ova vrsta poruke uključuje proslijeđene slike drugih Instagram profila. Link na post je pohranjen u stupcu `messages`. `("hscroll_share": > "target_url":)`
- CLIP: Odnosi se na proslijeđene video isječke s drugih Instagram profila. Da bi se pristupilo poveznici videozapisa, treba pretražiti stupac messages za određenu poruku. `("clip": > "clip": > "video_versions": > "url":)`
- PLACEHOLDER - Ako je izvorni profil s kojeg dolazi "XMA_MEDIA_SHARE ili CLIP" postavljen na privatno, poveznica prema mediju neće biti dostupna.

	thread_id	recipient_ids	timestamp	message_type	text	message
48	17103009491281398704 6638	324190	2023-06- 20:22:30	text		{"status":"UPLOADED","item_type":"text","item_i...
49	17103009491281398704 6638	324190	2023-07- 13:53:56	clip		{"status":"UPLOADED","item_type":"clip","item_id...
50	17103009491281398704 6638	324190	2023-07- 14:06:22	text		{"status":"UPLOADED","item_type":"text","item_i...
51	17103009491281398704 6638	324190	2023-07- 13:05:23	clip		{"status":"UPLOADED","item_type":"clip","item_id...
52	17103009491281398704 6638	324190	2023-07- 13:06:39	text		{"status":"UPLOADED","item_type":"text","item_i...
53	17103009491282017880 3765	229101	2023-06- 06:22:19	text		{"status":"UPLOADED","item_type":"text","item_i...
54	17103009491282017880 3765	229101	2023-07- 12:58:02	xma_media_share		{"status":"UPLOADED","item_type":"xma_media_...
55	17103009491282017880 3765	229101	2023-07- 13:03:52	clip		{"status":"UPLOADED","item_type":"clip","item_id...
56	17103009491282017880 3765	229101	2023-07- 13:04:20	text		{"status":"UPLOADED","item_type":"text","item_i...
57	17103009491282017880 3765	229101	2023-07- 13:04:27	text		{"status":"UPLOADED","item_type":"text","item_i...
58	17103009491282017880 3765	229101	2023-07- 13:04:47	text		{"status":"UPLOADED","item_type":"text","item_i...

Slika 10. Ispis Instagram poruka

Tijekom ovog detaljnog pregleda, moguće je efikasno dešifrirati i analizirati poruke, pružajući sveobuhvatan uvid u razmjenu informacija unutar razgovora na Instagramu.

6.1.3. Analiza podataka ekstrahiranih iz pretraživača Google Chrome

Analizirajući Google Chrome aplikaciju, uočava se nekoliko datoteka od interesa unutar direktorija `/com.android.chrome/app_chrome/Default`.

Datoteka `history` sadrži nekoliko ključnih tablica koje pružaju uvid u aktivnosti korisnika prilikom pretraživanja. Tablica `keyword_search_terms` bilježi pojmove koje je korisnik pretraživao, pružajući nam detalje o interesima i pretraživačkim navikama korisnika. Tablica `downloads` pohranjuje sve podatke o preuzetim datotekama koristeći preglednik.

S druge strane, tablica `urls` nije samo arhiva svih posjećenih web adresa, već također nudi bogatstvo dodatnih informacija o korisnikovim navikama pretraživanja. Osim što pohranjuje sve posjećene URL-ove, u stupcu `visit_count` može se proučiti koliko je puta korisnik posjetio određenu web stranicu, dok stupac `last_visit_time` bilježi datum i vrijeme posljednje

posjete toj stranici. Ovi podaci mogu biti korisni za razumijevanje učestalosti i posljednje interakcije korisnika s određenim web stranicama.

	id	url	title	visit_count	typed_count	last_visit_time	hidden
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
286	286	https://www.xda-developers.com/hp-...	HP EliteBook 800 G10 series: Price, release date,...	1	0	13332676841	0
287	287	https://www.hp.com/us-en/shop/pdp//pdp/hp-...	HP EliteBook 840 G10 Notebook PC - Customizable	9	0	13332621501	0
288	288	https://www.hp.com/us-en/shop/mdp/hp-...	HP EliteBook 840 | HP® Official Store	1	0	13332621501	0
289	289	https://www.hp.com/us-en/shop/mlp/hp-elite-...	HP Elite laptops | HP® Official Store	1	0	13332621511	0
290	290	https://www.hp.com/us-en/shop/mdp/hp-elite-...	HP EliteBook 1040 | HP® Official Store	1	0	13332621571	0
291	291	https://www.hp.com/us-en/shop/mdp/hp-elite-...	HP EliteBook 845 | HP® Official Store	1	0	13332621591	0
292	292	https://www.hp.com/us-en/shop/ConfigureView?...	HP Elitebook 845 G10 Notebook PC - Customizable	1	0	13332621621	0
293	293						0
294	294						0
295	295	https://www.google.com/search?...	wear os 4 - Google Search	2	0	13332676831	0
296	296	https://www.androidpolice.com/wear-os-4/	Wear OS 4: The next big smartwatch update ...	1	0	13332676801	0
297	297	https://www.google.com/search?...		1	0	13332724701	0
298	298						0
299	299						0
300	300						0
301	301						0

Slika 11. Prikazani podaci iz tablice `urls` u bazi podataka `history`

Datoteka `Bookmarks` služi za pohranjivanje svih "bookmarksa" ili obilježenih stranica koje korisnik smatra važnima. Za bolje razumijevanje strukture i informacija spremljenih u datoteci `Bookmarks`, razmatra se primjer jednog obilježenog linka::

```
"children": [ {
   "date_added": "13246352515164044",
   "date_last_used": "0",
   "guid": "2302834b-5d90-4418-b53e-a4cb3b4c83e8",
   "id": "42",
   "name": "FPZ - Zavod za informacijsko-komunikacijski promet",
   "type": "url",
   "url": "https://www.fpz.unizg.hr/ikp/index.php"
} ]
```

Datoteka `Cookies` u pregledniku Google Chrome igra ključnu ulogu u praćenju i pohranjivanju kolačića (engl. *cookies*) koje web stranice postavljaju na uređaj tijekom korisnikova pregledavanja interneta. Kolačići su datoteke koje web stranice koriste kako bi pohranile informacije na korisnikovom računalu. Ove informacije mogu se koristiti za različite svrhe, uključujući praćenje korisnikovih navika surfanja, zadržavanje prijave na web stranice i prilagodbu sadržaja ili oglasa korisniku.

`Login Data` datoteka čuva sve korisnikove spremljene podatke za prijavu, no treba napomenuti da lozinke nisu dostupne.

Posljednja datoteka, `Web Data`, pruža zanimljive uvide kroz nekoliko svojih tablica. Tablica `autofill` pohranjuje sve podatke koji su korisniku automatski popunjeni, kao i učestalost njihove upotrebe. Ako su korisnikove osobne informacije i adrese spremljene, one će se nalaziti u tablicama `local_addresses_type_tokens` i `server_addresses`.

Informacije o kreditnim karticama pohranjene su u tablici `masked_credit_card`. Ova tablica uključuje podatke kao što su ime na kartici u stupcu `name_on_card`, informacije o

platnoj mreži u stupcu `network`, zadnje četiri znamenke broja kartice u stupcu `last_four` te mjesec i godina isteka kartice u stupcima `exp_month` i `exp_year`.

6.1.4. Analiza podataka ekstrahiranih iz aplikacije Google Maps

Pri analizi aplikacije Google Maps, moguće je pristupiti ključnim informacijama vezanim za korisnikove pohranjene lokacije. Datoteka koja sadrži te informacije, `gmm_sync.db`, nalazi se u mapi `/com.google.android.apps.maps/databases/`.

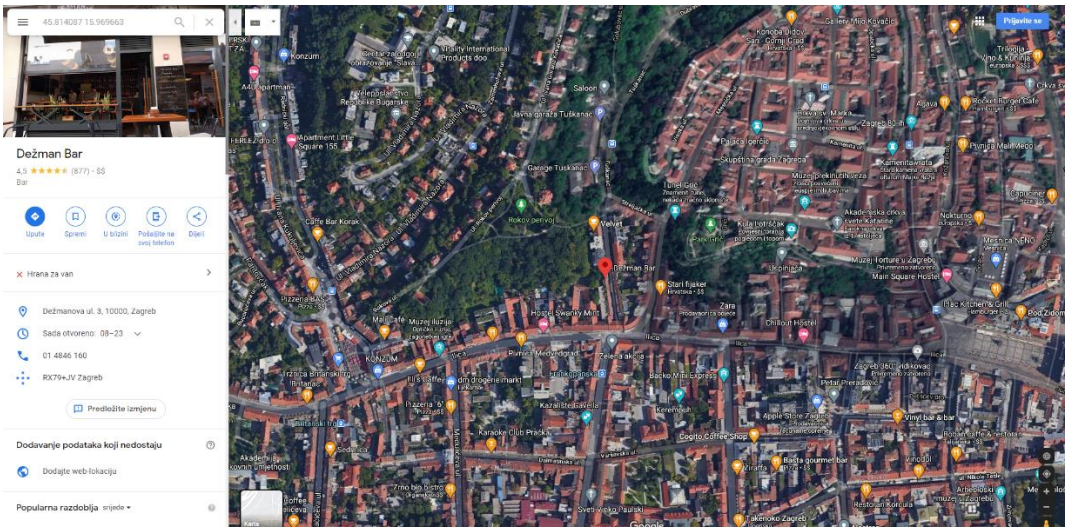
Unutar te baze, tablica `sync_item_data` posjeduje važne informacije. Stupac nazvan `timestamp` pokazuje kada je lokacija spremljena u Unix formatu vremena. Ovu vremensku oznaku može se pretvoriti u čitljiv format kako bi se dobila jasna predodžba kada je korisnik spremio određenu lokaciju.

Zemljopisne koordinate su ključne za svaku aplikaciju s mapama. U tablici, stupci pod nazivima `latitude_e6` i `longitude_e6` pružaju informacije o zemljopisnoj širini i dužini u mikrostupnjevima (otkud i "`e6`" u imenu). Te koordinate možemo unositi u Google Maps ili bilo koju drugu aplikaciju za mape, kako bi se dobila vizualna reprezentacija precizne lokacije koju je korisnik spremio.

Vizualni prikaz, kao što je slika s lokacijom, može dodatno objasniti kontekst, omogućujući korisnicima da bolje razumiju korisnikove aktivnosti na mapi. Važno je napomenuti da se pri pristupu ovim informacijama treba pridržavati svih pravila o zaštiti privatnosti.

timestamp	feature_fprint	latitude_e6	longitude_e6	
Filter	Filter	Filter	Filter	Filt
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	45814087	15969663	
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	

Slika 12. Baza podataka `gmm_sync.db`



Slika 13. Lokacija spremljene zemljopisne širine i dužine

Analiziranjem baze podataka `gmm_storage.db`, prvo što treba razmotriti je struktura i sadržaj tablica. Stupac `_key_pri` služi identifikaciji različitih vrsta podataka, dok drugi, poput `_data`, sadrži stvarne podatke.

Blob format, [20] u stupcu `_data` je format koji se često koristi za pohranu velikih količina binarnih ili tekstualnih podataka unutar baze podataka. Zbog svoje binarne prirode, takvi podaci obično nisu čitljivi kada se izravno pregledavaju unutar baze. Da bi razumjeli sadržaj, potrebno je izvući blob podatke i pregledati ih pomoću alata koji može interpretirati binarne podatke, poput hex preglednika Hxd, [21].

U stupcu `_key_pri` moguće je prepoznati vrstu lokacije. Unos `bundled` u tom stupcu sugerira da predstavlja rezultate pretraživanja, [5], dok unos `uri` ukazuje na konkretne lokacije do kojih je usmjerena navigacija, zajedno s detaljnim putem navigacije.

	_key_pri ▲1	_key_sec	_data
	Filter	Filter	Filter
110	bundled	349	BLOB
111	bundled	348	BLOB
112	bundled	347	BLOB
113	bundled	346	BLOB
114	bundled	345	BLOB

Slika 14. Baza podataka `gmm_storage.db`

```
00000310  30 65 64 37 35 36 64 35 36 64 63 66 1A 1A 5A 6C  0ed756d56dcf..Zl
00000320  61 74 6E 69 20 56 72 74 20 28 47 6F 6C 64 65 6E  atni Vrt (Golden
00000330  20 47 61 72 64 65 6E 29 22 0E 42 6F 72 65 6C 6C   Garden)".Borell
00000340  69 20 75 6C 2E 20 31 32 22 0C 32 33 30 30 30 2C  i ul. 12".23000,
00000350  20 5A 61 64 61 72 32 F5 0F 1A 6A 1A 06 E2 82 AC   Zadar2õ..j..â,¬
```

Slika 15. Ispis 110. `Bundled blob` zapisa iz slike

6.1.5. Analiza podataka ekstrahiranih iz aplikacije Kalendar

Analizirajući bazu podataka kalendara, može se pristupiti svim evidentiranim događanjima i detaljnim opisima povezanim s njima. Relevantna datoteka, nazvana `calendar.db`, nalazi se u direktoriju `/com.android.providers.calendar/databases`. Ova baza podataka sadrži pogled (engl. *view*) imenovan `view_events`, koji obuhvaća sve događaje i pripadajuće informacije. Dakle, analiza ovog pogleda sastoji se od prilagodbe upita kako bi obuhvatio relevantne stupce koje želimo istražiti.

Stupac `title` sadrži nazive svih pohranjenih događaja. Ako je za događaj definirana lokacija, ona će biti pohranjena u stupcu `eventLocation`. Stupci `dtstart` i `dtend` dokumentiraju planirano vrijeme početka i kraja događaja. Stupac `account_name` otkriva korisnički račun u kojem je događaj pohranjen. Stupac `calendar_displayName` prikazuje ime korisničkog računa koji je stvorio događaj ili vrstu događaja, ako je takva dodijeljena.

	_id	title	eventLocation	DTStart	DTEnd	calendar_id	account_name	calendar_displayName
11	11			2023-01-0 06:35:00	2023-01-0 07:35:00	3	@gmail.com	@gmail.com
12	12			2023-01-0 17:35:00	2023-01-0 18:35:00	3	@gmail.com	@gmail.com
13	13			2023-04-1 06:00:00	2023-04-1 07:00:00	3	@gmail.com	@gmail.com
14	14			2023-03-2 15:30:00	2023-03-2 16:30:00	3	@gmail.com	@gmail.com
15	15			2023-02-1 15:20:00	2023-02-1 16:20:00	3	@gmail.com	@gmail.com
16	16			2023-04-2 08:40:00	2023-04-2 09:40:00	3	@gmail.com	@gmail.com
17	17			2023-05-2 16:20:00	2023-05-2 17:20:00	3	@gmail.com	@gmail.com
18	18							
19	19			2023-10-1 00:00:00	NULL	2	@gmail.com	Birthdays
20	20							
21	21			2018-02-1 00:00:00	NULL	2	@gmail.com	Birthdays
22	22			2019-06-2 00:00:00	NULL	2	@gmail.com	Birthdays
23	23			2019-09-0 00:00:00	NULL	2	@gmail.com	Birthdays
24	24			2019-12-2 00:00:00	NULL	2	@gmail.com	Birthdays
25	25			2023-07-0 16:50:00	2023-07-0 17:50:00	3	@gmail.com	@gmail.com
26	26		Ljubljana, 1000, Slovenia	2023-05-1 00:00:00	2023-05-1 00:00:00	5	@gmail.com	@gmail.com
27	27			2023-06-3 04:30:00	2023-06-3 05:30:00	3	@gmail.com	@gmail.com
28	98			2023-07-0 08:15:00	2023-07-0 09:15:00	3	@gmail.com	@gmail.com
29	99			2023-07-1 08:00:00	2023-07-1 09:00:00	3	@gmail.com	@gmail.com

Slika 16. Baza podataka `calendar.db`

6.1.6. Analiza podataka ekstrahiranih iz SMS poruka

Kroz analizu baza podataka aplikacije Google Messages, koja služi za slanje SMS poruka, dobiva se uvid u sve razgovore i poruke. Baza podataka koja čuva ove informacije imenovana je kao `bugle_db` i može se pronaći unutar mape `/com.google.android.apps.messaging/databases`.

Ova baza podataka sadrži dvije ključne tablice: `conversations` i `parts`. Tablica `conversations` je posvećena arhiviranju svih razgovora. Konkretno, imena kontakata ili brojevi s kojima su razgovori vođeni, spremljeni su u stupcu pod nazivom `name`, dok se zadnja poslana ili primljena poruka u konverzaciji može naći u stupcu `snippet_text`.

S druge strane, tablica `parts` sadrži zbirku svih poslanih poruka. Tekst svake poruke je pohranjen u stupcu `text`, dok se vremenska oznaka primanja ili slanja poruke nalazi u stupcu

timestamp. Kao Android sustavi su temeljeni na Linux kernelu, koriste se s Unix vremenom, stoga brojevi u stupcu timestamp prikazuju vrijeme kada je poziv ostvaren, prema Unix vremenskoj skali.

U analitičkom procesu, izrađen je prilagođeni SQL upit koji spaja dvije tablice, conversations i parts, iz baze podataka. Ovaj upit pruža učinkovit način da povežem sve poruke s njihovim odgovarajućim conversation_id, rezultirajući detaljnim prikazom svih poruka unutar pojedinačnog razgovora.

SQL upit prikazan je ispod:

```
SELECT  CONV._id
       ,PART.conversation_id
       ,PART.text
       ,DATETIME(PART.timestamp/1000,'unixepoch') AS 'DateTime'
       ,CONV.name
FROM main.parts AS PART
INNER JOIN main.conversations AS CONV
  ON CONV._id = PART.conversation_id
ORDER BY CONV._id ASC
```

Ovaj upit odabire stupce _id, conversation_id i text iz tablice parts, kao i DateTime (koji predstavlja formatirano vrijeme poruke) i name iz tablice conversations. Koristi se INNER JOIN operacija kako bi se spojile ove dvije tablice na temelju zajedničkog stupca _id iz conversations i conversation_id iz parts. Rezultati su potom sortirani prema _id stupcu iz conversations. Na ovaj način, prikaz svih poruka unutar nekog razgovora je organiziran i lako dostupan kao što se vidi iz slike ispod.

	_id	conversation_id	text	DateTime	name
13	7	7	To log in to your account, use this code: [redacted].	2023-07-1[redacted] 17:0[redacted]	SMSinfo
14	8	8	eBay: Your security code is [redacted]. Do not share...	2023-06-2[redacted] 10:0[redacted]	+4[redacted]
15	9	9	[redacted]	2023-06-2[redacted] 08:5[redacted]	091[redacted]
16	9	9	[redacted]	2023-06-2[redacted] 08:5[redacted]	091[redacted]
17	9	9	[redacted]	2023-06-2[redacted] 09:1[redacted]	091[redacted]
18	10	10	Posiljka [redacted] je utovarena za dostavu. ...	2023-06-2[redacted] 06:3[redacted]	092[redacted]
19	11	11	[redacted] is your Google verification code.	2023-06-2[redacted] 08:3[redacted]	Google
20	11	11	[redacted] is your Google verification code.	2023-06-2[redacted] 08:3[redacted]	Google
21	12	12	[redacted] is your Google verification code.	2023-07-0[redacted] 12:3[redacted]	Google
22	12	12	[redacted] is your Google verification code.	2023-07-0[redacted] 15:2[redacted]	Google
23	12	12	[redacted] is your Google verification code.	2023-07-0[redacted] 08:1[redacted]	Google
24	12	12	[redacted] je vaš kontrolni kôd za Google.	2023-07-0[redacted] 11:4[redacted]	Google
25	12	12	[redacted] is your Google verification code.	2023-07-0[redacted] 10:2[redacted]	Google
26	12	12	[redacted] is your Google verification code.	2023-07-0[redacted] 08:0[redacted]	Google
27	12	12	[redacted] is your Google verification code.	2023-07-1[redacted] 16:0[redacted]	Google
28	12	12	[redacted] is your Google verification code.	2023-07-1[redacted] 10:3[redacted]	Google
29	13	13	Nazvat ću kasnije.	2023-07-0[redacted] 13:0[redacted]	[redacted]
30	13	13	[redacted]	2023-07-0[redacted] 13:0[redacted]	[redacted]
31	13	13	[redacted]	2023-07-0[redacted] 13:2[redacted]	[redacted]
32	14	14	Posiljka [redacted] je utovarena za dostavu. ...	2023-07-0[redacted] 05:4[redacted]	092[redacted]

Slika 17. Ispis upita na bazu podataka Google Messages aplikacije

6.1.7. Analiza podataka ekstrahiranih iz kontakta i popisa poziva

Istraživanjem baza podataka aplikacije Google Dialer mogu se prikupiti informacije o svim brojevima pohranjenim na uređaju. Baza podataka koja čuva te informacije naziva se `dialer.db` i može se pronaći u mapi `/com.google.android.dialer/databases/`.

Baza podataka `dialer.db` sadrži ključnu tablicu `smartdail_tablu`. U stupcu `phone_number` vidljivi su svi brojevi pohranjeni na mobilnom uređaju, dok stupac `display_name` prikazuje imena dodijeljena svakom pojedinom broju.

Podaci o pozivima pohranjeni su u istom direktoriju, ali u različitoj datoteci, imenovanoj `annotated_call_log.db`. Tablica `AnnotatedCallLog` sadrži ključne stupce, `formatted_number` koji prikazuje brojeve s kojima dolazi ili na koje odlazi poziv, dok stupac `duration` navodi vremensko trajanje svakog poziva.

Stupac `call_type` sadrži vrijednosti u rasponu od 1 do 7, pri čemu svaki broj predstavlja različitu vrstu poziva.

call_type	**Opis**
1	Dolazni poziv
2	Odlazni poziv
3	Propušteni poziv
4	Govornu poštu
5	Odbijen poziv
6	Poziv blokiranog broja
7	Poziv na koji je odgovoreno na drugom uređaju

Tablica 3. Opis `call_type` vrijednosti

Kao dopunu svom istraživačkom procesu, kreirao sam prilagođeni SQL upit koji povezuje tablicu `AnnotatedCallLog` iz datoteke `annotated_call_log.db` i tablicu `smartdial_table` iz datoteke `dialer.db`.

SQL upit prikazan je ispod:

```
SELECT  DATETIME(timestamp/1000,'unixepoch') AS 'DateTime'
       ,formatted_number
       ,TIME(duration,'unixepoch') AS 'Call Duration'
       ,phone_account_id
       ,call_type
       ,display_name
FROM annotated_call_log.AnnotatedCallLog AS 'CallLogs'
LEFT JOIN smartdial_table AS 'Contacts'
  ON CallLogs.formatted_number = Contacts.phone_number
```

Ovaj upit odabire stupce `DateTime` (koji predstavlja formatirano vrijeme poziva), `formatted_number`, `Call Duration` (koji prikazuje trajanje poziva u prikladnom formatu), `phone_account_id` koji prikazuje koja je SIM kartica korištena prilikom poziva, `call_type`

iz tablice `AnnotatedCallLog`, kao i `display_name` iz tablice `smartdial_table`. Koristi se `LEFT JOIN` operacija kako bi se spojile ove dvije tablice temeljem zajedničkog broja telefona.

Kroz ovaj upit, moguće je dobiti jasan i strukturiran pregled svih dolaznih poziva, s tim da imena kontakata u stupcu `display_name` neće uvijek biti dostupna ako broj nije pohranjen u kontaktima kao što se vidi iz slike ispod.

	DateTime	formatted_number	Call Duration	phone_account_id	call_type	display_name
13	2023-06-26 13:04:49	+385 91 46	00:00:47	2	1	NULL
14	2023-06-27 07:41:29	+385 91 46	00:00:34	2	2	
15	2023-06-27 12:20:38	+385 99 59	00:00:28	1	1	
16	2023-06-28 06:51:54	+385 91 46	00:00:00	2	3	
17	2023-06-28 06:55:00	+385 91 46	00:00:00	1	2	
18	2023-06-28 08:02:29	+385 91 49	00:00:18	2	2	NULL
19	2023-06-28 08:58:54	+385 91 46	00:00:09	2	2	Matija
20	2023-06-28 08:59:24	+385 91 46	00:00:00	2	5	NULL
21	2023-06-28 11:53:20	+385 91 46	00:01:31	2	1	NULL
22	2023-06-28 12:18:08	+385 99 40	00:00:10	1	1	Josip
23	2023-06-29 07:04:18	+385 91 95	00:00:14	1	1	NULL
24	2023-06-29 09:09:04	+385 99 59	00:00:13	1	1	NULL

Slika 18. Ispis poziva i kontakta

6.2. Analiza direktno dostupnih podataka s uređaja

Jedan od ključnih koraka u forenzičkoj analizi Android uređaja je ispitivanje direktno dostupnih podataka, koji mogu pružiti brz i neposredan uvid u aktivnosti korisnika, kao i potencijalne dokaze relevantne za istragu.

6.2.1. Sustavni logovi

Logovi su značajan izvor informacija prilikom forenzičke analize bilo kojeg operativnog sustava, pa tako i Androida. Sustavni logovi, poznati kao *logcat*, zapisuju različite informacije o događajima, postupcima i problemima unutar sustava. Prikupljajući te logove, analitičar može dobiti uvid u različite aspekte uređaja, od jednostavnih operacija aplikacija do potencijalno sumnjivih ili malicioznih aktivnosti.

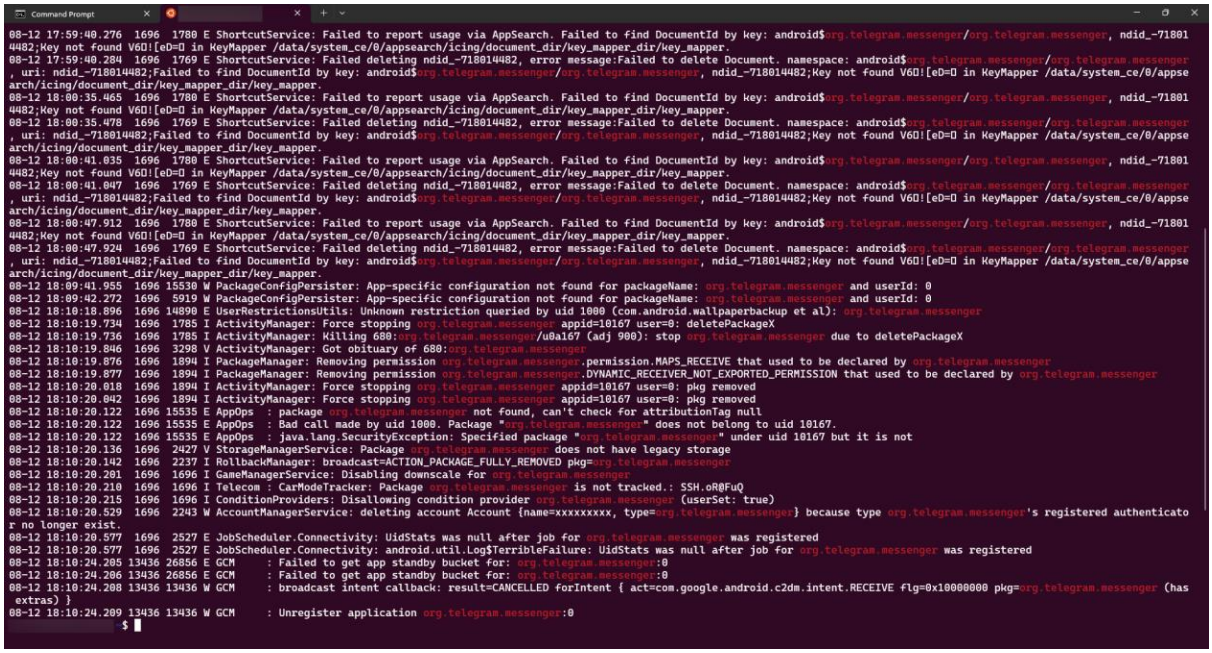
Koristeći naredbu `adb logcat`, moguće je dohvatiti sustavne logove s uređaja u stvarnom vremenu. Ova naredba omogućava filtriranje informacija kako bi se usmjerila pažnja na određene komponente ili događaje, [22].

Osim što pružaju informacije o radu uređaja, sustavni logovi mogu sadržavati razne informacije o:

- Instalaciji ili deinstalaciji aplikacija.
- Mrežnoj aktivnosti i povezivanju na različite Wi-Fi mreže.
- Porukama o pogreškama ili padovima aplikacija.
- Sumnjivim ili neobičnim aktivnostima koje se mogu povezati s malverom ili drugim napadima.

Pregledom logcat zapisa primjećujemo da je aplikacija Telegram bila izbrisana neposredno prije provedbe forenzičke analize uređaja:

```
>adb logcat -d > \\wsl.localhost\Ubuntu\home\user\logcat.txt
user@ubuntu-pc:~$ cat logcat.txt | grep "org.telegram.messenger"
```



Slika 19. Primjer `logcat` ispisa

Analitičar može prilagoditi naredbe kako bi fokusirao pretragu i proučavao specifične događaje ili aktivnosti. Međutim, važno je napomenuti da se logovi s vremenom brišu kako bi se oslobodio prostor za nove zapise. Stoga, u kontekstu forenzičke analize, važno je što prije prikupiti logove kako bi se osigurao što potpuniji skup podataka.

6.2.2. WiFi SSID i lozinke

Poznavanje mreža na koje je Android uređaj bio spojen može biti ključno za forenzičku analizu. Ove informacije ne samo da otkrivaju s kojim mrežama je korisnik bio povezan, već mogu pružiti dodatne podatke koji se odnose na korisnikove lokacije, navike ili druge uređaje s kojima su bili povezani. Pored samih naziva mreža (SSID), veoma vrijedna informacija je i lozinka koju je korisnik koristio za pristup tim mrežama.

Jedna od ključnih datoteka koja sadrži informacije o Wi-Fi konfiguracijama je `WifiConfigStore.xml`. Ova datoteka sadrži mnoge konfiguracijske parametre vezane za Wi-Fi, uključujući SSID-ove i lozinke.

Da bi se izvukle samo relevantne informacije iz ove datoteke, sljedeća komanda se može koristiti:

```
haydn:/ # cat /data/misc/apexdata/com.android.wifi/WifiConfigStore.xml |
grep -E '"PreSharedKey"|"SSID"'
```

```
<string name="SSID">&amp;quot;Galaxy S21+ 5G&amp;quot;</string>
<string name="PreSharedKey">&amp;quot;mhwc2788&amp;quot;</string>
<string name="SSID">&amp;quot;SSIDExample&amp;quot;</string>
<string name="PreSharedKey">&amp;quot;2sZTsB5Cak&amp;quot;</string>
```

6.2.3. IMEI uređaja

IMEI (engl. *International Mobile Equipment Identity*) je jedinstveni identifikacijski broj dodijeljen svakom mobilnom uređaju, i služi kao njegov "otisak prsta". Pomoću IMEI-a, operateri mreže mogu identificirati svaki uređaj unutar svoje mreže i pratiti ga za različite svrhe, uključujući zaštite od krađe. U kontekstu forenzičke analize, IMEI je ključna informacija jer može pomoći u utvrđivanju povijesti uređaja, njegovih prethodnih vlasnika i potencijalnih zloupotreba.

Da bi se koristeći ADB shell dohvatio IMEI broj uređaja, sljedeća naredba se može upotrijebiti:

```
haydn:/ # service call iphonesubinfo 1 s16 com.android.shell
```

```
Result: Parcel(
  0x00000000: 00000000 0000000f 00360038 00390035 '........8.6.5.9.'
  0x00000010: 00300037 00350030 00380034 00340031 '7.0.0.5.4.8.1.4.'
  0x00000020: 00310039 00000036                   '9.1.6...        ')
```

```
haydn:/ # service call iphonesubinfo 1 s16 com.android.shell
```

```
Result: Parcel(
  0x00000000: 00000000 0000000f 00360038 00390035 '........8.6.5.9.'
  0x00000010: 00300037 00350030 00380034 00340031 '7.0.0.5.4.8.1.4.'
  0x00000020: 00300039 00000038                   '9.0.8...        ')
```

Ova naredba poziva servis koji je zadužen za pružanje informacija o telefonu i zahtijeva IMEI broj za specifičnu SIM karticu. Ako uređaj podržava korištenje više SIM kartica, potrebno je prilagoditi naredbu (promjenom broja koji se nalazi iza `iphonesubinfo`) kako bi se dobio IMEI za svaku od njih.

6.2.4. Povijest SIM kartica korištenih u uređaju

Prema izvoru [23], da bi se analizirale informacije o SIM karticama koje su korištene u Android uređaju, može se upotrijebiti sljedeća naredba:

```
haydn:/ # sqlite3 -line /data/user_de/0/com.android.providers.telephony/
databases/telephony.db SELECT icc_id,card_id,carrier_name,display_name,
mcc,mnc FROM siminfo'
      icc_id = 8938591421XXXXXXXXX
     card_id = 8938591421XXXXXXXXXF
carrier_name = A1 HR
display_name = A1 Personal
         mcc = 219
         mnc = 10

      icc_id = 8938591416XXXXXXXXX
     card_id = 8938591416XXXXXXXXXF
carrier_name = A1 HR
display_name = A1 Work
         mcc = 219
         mnc = 10

      icc_id = 8938591421XXXXXXXXX
     card_id = 8938591421XXXXXXXXXF
carrier_name = A1 HR
display_name = A1 TestSIM
         mcc = 219
         mnc = 10
```

Navedena naredba pruža pristup bazi podataka u kojoj su pohranjene informacije o SIM karticama. Iz te baze mogu se dobiti podaci poput ID-a SIM kartice (`icc_id`), ime operatera (`carrier_name`), ime za prikaz (`display_name`) te MCC (`mcc`) i MNC (`mnc`).

Putem ovih informacija, postaje moguće stvoriti cjelovitu sliku o upotrebljenim SIM karticama. Ovo može biti presudno pri rekonstrukciji povijesti korištenja uređaja, identificiranju mreža i operatera s kojima je uređaj bio povezan, kao i ostalim aspektima koji su od značaja za forenzičku analizu.

6.2.5. Uvid u korištenje aplikacija

`dumpsys usagestats` je alat unutar Android operativnog sustava koji nudi duboki uvid u korištenje aplikacija na uređaju. Pružajući forenzičkim analitičarima dragocjene informacije, ovaj alat može otkriti mnogo više od puke povijesti uporabe aplikacija.

1. **Vremenski tragovi**: Jedan od najkorisnijih aspekata dumpsys usagestats je mogućnost prikaza točnog vremena kada je određena aplikacija pokrenuta ili zatvorena. To pomaže analitičarima rekonstruirati aktivnosti korisnika u određenom vremenskom periodu.
2. **Frekvencija uporabe**: Pored samih vremenskih tragova, dumpsys usagestats može otkriti i koliko često je određena aplikacija korištena. Ako, na primjer, sumnjiva aplikacija pokazuje visoku frekvenciju uporabe, to može biti indikacija maliciozne aktivnosti.
3. **Detalji o interakcijama**: Alat ne pruža samo informacije o tome kada je aplikacija bila otvorena, već i o tome kako je korištena, uključujući događaje poput klikova i interakcija s obavijestima.

Na temelju odabranog datuma koji je od značaja za istragu, prikazuju se rezultati analize aplikacije Telegram:

```
haydn:/ # dumpsys usagestats | grep "org.telegram.messenger" | grep "2023-08-09"
    package=org.telegram.messenger   totalTimeUsed="00:20"   lastTimeUsed="2023-08-09 23:40:34" appLaunchCount=2
```

Razumijevanje ovih informacija omogućava analitičarima da steknu cjelovitu sliku o aktivnostima korisnika na uređaju, što može biti ključno za razumijevanje ponašanja, motivacija i eventualnih prijetnji.

7. Zaključak

U današnje doba gdje tehnologija napreduje nevjerojatnom brzinom, pametni telefoni nisu samo uređaji za komunikaciju, već i generiraju veliku količinu informacija o svakodnevnim aktivnostima korisnika. Rad je pružio duboko razumijevanje arhitekture sustava Android, čime je istaknuta važnost svake komponente u okviru operativnog sustava. Njegovo značenje ne leži samo u funkcionalnosti, već i u tome kako se podaci pohranjuju, kako su zaštićeni i kako ih je moguće ekstrahirati.

Forenzička analiza, kao disciplina, postala je neophodna u suvremenim pravosudnim postupcima, posebno kada su u pitanju digitalni tragovi. Da bi takva analiza bila uspješna, od presudne je važnosti razumijevanje metoda ekstrakcije podataka s Android uređaja. Raznolikost alata koji su na raspolaganju forenzičarima, njihova specifična uporaba, prednosti i nedostaci, ključni su za donošenje ispravne odluke o tome koji alat koristiti za određenu vrstu analize.

Pri analizi samih podataka, važnost preciznosti i detalja ne može se dovoljno naglasiti. Kroz upotrebu specifičnih alata, poput ADB i DB Browser for SQLite, forenzičari imaju priliku ne samo pregledavati podatke, već i formatirati ih na način koji omogućuje lakše razumijevanje i interpretaciju. Ova sposobnost prevođenja sirovih podataka u smislene informacije ono je što često razdvaja kvalitetne od ne kvalitetnih forenzičkih analiza.

Kroz detaljnu analizu i interpretaciju forenzičke analize Android uređaja, ovaj rad potvrđuje kako su tehnologija i pravosudni postupci neraskidivo povezani. Dok tehnologija nastavlja napredovati, izazovi s kojima se suočavaju forenzičari postaju sve složeniji. Stoga je od presudne važnosti da se stručnjaci u ovom području neprestano obrazuju i prilagođavaju, kako bi ostali korak ispred potencijalnih prepreka i izazova koji se postavljaju pred njih.

Literatura

[1] Android Source. https://source.android.com/docs/setup/about [Pristupljeno: Kolovoz 2023.]

[2] Android Source. https://source.android.com/docs/security/overview [Pristupljeno: Kolovoz 2023.]

[3] Tamma R., Skulkin O., Mahalik H. Bommisetty S. *Practical Mobile Forensics - Fourth Edition*; Packt Publishing; 2020.

[4] Android Source. Preuzeto sa: https://source.android.com/docs/core/architecture [Pristupljeno: Kolovoz 2023.]

[5] Skulkin O, Tindall D., Tamma R. *Learning android forensics: Analyze android devices with the latest forensic tools and Techniques*; Packt Publishing; 2018.

[6] Statcounter. Preuzeto sa: https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-200901-202308 [Pristupljeno: Kolovoz 2023.]

[7] Cencenelece.eu. Preuzeto sa: https://www.cencenelec.eu/news-and-events/news/2022/eninthespotlight/2022-04-12-for-mobile/ [Pristupljeno: Srpanj 2023.]

[8] INTERPOL. Global guidelines for digital forensics laboratories. Preuzeto sa: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf [Pristupljeno: Srpanj 2023.]

[9] Tadviser. Preuzeto sa: https://tadviser.com/index.php/Company:Cellebrite_Mobile_Synchronization [Pristupljeno: Kolovoz 2023.]

[10] NewTechSystem. Preuzeto sa: https://www.newtechsystem-recuperodati.com/chip-off.html [Pristupljeno: Kolovoz 2023.]

[11] Cellebrite. Preuzeto sa: https://cellebrite.com/en/ufed/ [Pristupljeno: Kolovoz 2023.]

[12] Oxygen Forensics. Preuzeto sa: https://oxygenforensics.com/en/ [Pristupljeno: Kolovoz 2023.]

[13] Android Developers. Preuzeto sa: https://developer.android.com/tools/adb [Pristupljeno: Kolovoz 2023.]

[14] Autopsy. Preuzeto sa: https://s3.amazonaws.com/resources.autopsy.com/datasheets/Autopsy-EN.pdf [Pristupljeno: Kolovoz 2023.]

[15] Autopsy User Documentation. Preuzeto sa: http://sleuthkit.org/autopsy/docs/user-docs/4.21.0//android_analyzer_page.html [Pristupljeno: Kolovoz 2023.]

[16] Autopsy User Documentation. Preuzeto sa: http://sleuthkit.org/autopsy/docs/user-docs/4.21.0//aleapp_page.html [Pristupljeno: Kolovoz 2023.]

[17] Github. Preuzeto sa: https://github.com/sqlitebrowser/sqlitebrowser [Pristupljeno: Kolovoz 2023.]

[18] Statista. Preuzeto sa: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ [Pristupljeno: Kolovoz 2023.]

[19] Comment Picker. Preuzeto sa: https://commentpicker.com/instagram-username.php [Pristupljeno: Kolovoz 2023.]

[20] Oracle Docs. Preuzeto sa: https://docs.oracle.com/javadb/10.8.3.0/ref/rrefblob.html [Pristupljeno: Kolovoz 2023.]

[21] HxD. Preuzeto sa: https://mh-nexus.de/en/hxd/ [Pristupljeno: Kolovoz 2023.]

[22] Android Developers. Preuzeto sa: https://developer.android.com/tools/logcat [Pristupljeno: Kolovoz 2023.]

[23] StackExchange. Preuzeto sa: https://android.stackexchange.com/questions/217830/how-to-check-imsi-iccid-on-miui10 [Pristupljeno: Kolovoz 2023.]

Popis kratica

ADB	Android Debug Bridge
AOSP	Android Open Source Project
API	Application Programming Interface
FSD	File System Dump
GPS	Global Positioning System
HAL	Hardware Abstraction Layer
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
MCC	Mobile Country Code
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
OEM	Original Equipment Manufacturer
PDF	Portable Document Format
SIM	Subscriber Identity Module
SMS	Short Message Service
SQL	Structured Query Language
SSID	Service Set Identifier
UFED	Universal Forensic Extraction Device
VPN	Virtual Private Network

Popis slika

Popis grafova

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je **završni rad** 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 **Forenzička analiza pametnog Android telefona**, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 4.9.2023.

Ivan Barišić Ivan Barišić

(ime i prezime, *potpis*)