A logo with text and hands

Description automatically generated with medium confidenceA blue and white logo

Description automatically generated

**Univerzitet u Nišu**

**Elektronski faktultet**

**Forenzika Android mobilnih uredjaja**

Studijski program: Računarstvo i informatika

Modul: Softversko inženjerstvo

Student: Profesor:

Katarina Maksimović, 1599 Prof. dr. Bratislav Predić

Niš, April 2024. godina

Sadržaj

[1. Uvod 3](#_Toc161507689)

[2. Osnove Android operativnog sistema 3](#_Toc161507690)

[2.1. Struktura Android datotečnog sistema i važnih direktorijuma 5](#_Toc161507691)

[3. Metodologija digitalne forenzike 7](#_Toc161507692)

[3.1. Opis forenzičkih koraka 8](#_Toc161507693)

[4. Alati i tehnike za forenzičku analizu Android uređaja 9](#_Toc161507694)

[5. Forenzička analiza mobilnih aplikacija 11](#_Toc161507695)

[5.1. Proces ekstrakcije korisnih informacija iz APK datoteka 13](#_Toc161507696)

[6. Analiza podataka i korisničkih informacija 14](#_Toc161507697)

[7. Android Debug Bridge (ADB) 19](#_Toc161507698)

[8. Zaključak 26](#_Toc161507699)

[9. Literatura 27](#_Toc161507700)

# Uvod

Digitalna forenzika predstavlja ključan aspekt savremene istraživačke prakse, naročito u kontekstu mobilnih uređaja. Digitalna forenzika se odnosi na disciplinu koja se bavi identifikacijom, prikupljanjem, analizom i interpretacijom digitalnih dokaza radi rešavanja kriminalnih dela i pružanja podrške pravosudnim procesima. Mobilni uređaji, posebno Android uređaji, postali su neizostavan deo svakodnevnog života, čuvajući ogromne količine podataka koji mogu biti od ključnog značaja za istražne postupke.

Forenzičke analize mobilnih uređaja, a posebno Android uređaja, imaju veliku važnost u istrazi kriminalnih dela i pružanju pravde. Podaci sa ovih uređaja mogu pružiti ključne informacije o aktivnostima pojedinaca, komunikaciji, lokacijama, finansijskim transakcijama i drugim relevantnim informacijama koje su od vitalnog značaja za istragu. Forenzička analiza Android uređaja obuhvata širok spektar tehnika i alata za prikupljanje, analizu i interpretaciju podataka sa uređaja.

U ovom radu, fokus će biti stavljen na forenzičku analizu Android mobilnih uređaja. Biće istraženi različiti aspekti forenzičkih analiza, uključujući metodologiju, alate, tehnike i izazove. Cilj je pružiti dublje razumevanje procesa forenzičke analize mobilnih uređaja, posebno Android uređaja, kako bi se omogućila efikasna identifikacija i interpretacija digitalnih dokaza u istražnim postupcima i pravosudnim procesima.

# Osnove Android operativnog sistema

Android operativni sistem je operativni sistem razvijen od strane kompanije Google, koji je namenjen za uređaje kao što su pametni telefoni, tableti, pametni satovi i drugi slični uređaji. On je postao izuzetno popularan zbog svoje fleksibilnosti, prilagodljivosti i širokog spektra funkcionalnosti.

Android operativni sistem je baziran na Linux kernelu, što pruža osnovni nivo stabilnosti i sigurnosti. Međutim, Android se razlikuje od klasičnih Linux distribucija zbog svoje arhitekture i načina na koji je organizovan. Arhitektura Androida se sastoji od više slojeva, uključujući Linux kernel, Android Runtime (ART), Java API framework, System Libraries, Application Framework, i Applications. Ovi slojevi rade zajedno kako bi pružili okruženje u kojem aplikacije mogu da funkcionišu i korisnici da interaguju sa uređajem.

Svaki od slojeva u arhitekturi Android operativnog sistema ima svoju specifičnu ulogu i doprinosi funkcionisanju sistema kao celine. Sledi detaljniji opis svakog sloja:

1. Linux kernel:

* Linux kernel je srce Android operativnog sistema. To je komponenta koja upravlja hardverom uređaja i pruža osnovne funkcionalnosti kao što su upravljanje memorijom, upravljanje procesima, upravljanje uređajima, bezbednost i druge operativne zadatke.
* Linux kernel omogućava Androidu da efikasno komunicira sa hardverom uređaja, uključujući ekran, kameru, senzore, bateriju i druge komponente.

1. Android runtime (ART):

* Android runtime (ART) je okruženje za izvršavanje aplikacija na Androidu. ART prevodi Java bytecode aplikacija u mašinski kod koji može direktno izvršavati procesor uređaja.
* ART zamjenjuje prethodni JIT (Just-In-Time) kompilator, što rezultira bržim i efikasnijim izvršavanjem aplikacija.

1. Java API framework:

* Java API framework pruža programski interfejs za razvoj Android aplikacija koristeći Java programski jezik.
* Ovaj sloj sadrži veliki broj različitih API-ja koji omogućavaju pristup različitim funkcijama i servisima uređaja, uključujući upravljanje korisničkim interfejsom, pristup bazi podataka, mrežne operacije, senzore, lokaciju i mnoge druge.

1. System libraries:

* System libraries su skup biblioteka koje pružaju osnovne funkcionalnosti Android operativnog sistema. Ove biblioteke omogućavaju različite zadatke kao što su upravljanje podacima, obrada slika, audio reprodukcija, mrežne operacije i mnoge druge.
* System Libraries su deo Android SDK (Software Development Kit) i koriste se prilikom razvoja aplikacija.

1. Application framework:

* Application framework je sloj koji pruža infrastrukturu za razvoj Android aplikacija. On uključuje različite komponente i servise kao što su Activity Manager, Content Providers, Resource Manager, Notification Manager i druge.
* Ovi servisi omogućavaju kreiranje različitih vrsta aplikacija, upravljanje životnim ciklusom aplikacija, pristup deljenim resursima, upravljanje obaveštenjima i druge funkcionalnosti.

1. Applications:

* Applications su krajnje aplikacije koje se izvršavaju na Android uređaju. To su aplikacije koje korisnici preuzimaju i instaliraju sa Google Play Store-a ili drugih izvora.
* Ove aplikacije mogu biti različitih vrsta, uključujući aplikacije za komunikaciju, društvene mreže, produktivnost, igre, multimediju i mnoge druge.

Android nudi širok spektar funkcionalnosti koje su dizajnirane da poboljšaju korisničko iskustvo. To uključuje korisnički interfejs koji je prilagodljiv i intuitivan za korišćenje, podršku za različite vrste aplikacija koje se mogu preuzeti sa Google Play Store-a ili drugih izvora, mogućnost povezivanja sa različitim mrežama i uređajima putem Wi-Fi, Bluetooth, mobilnih mreža, NFC i USB, kao i reprodukciju multimedijalnog sadržaja kao što su muzika, video i fotografije. Takođe, Android korisnicima omogućava veliku personalizaciju uređaja, uključujući promenu pozadine ekrana, izbor tema, prilagođavanje rasporeda aplikacija i drugih podešavanja.

# 2.1. Struktura Android datotečnog sistema i važnih direktorijuma

Android datotečni sistem organizuje i čuva podatke na uređaju. Osnovna struktura Android datotečnog sistema je bazirana na Linux datotečnom sistemu, obično Ext4. Datotečni sistem je podeljen na različite particije, od kojih svaka ima svoju specifičnu svrhu. Neke od particija Android datotečnog sistema su:

A screenshot of a computer

Description automatically generated

Slika 1. Struktura Android datotečnog Sistema

1. /system:

Ovaj direktorijum sadrži osnovni operativni sistem i sistemske aplikacije. To uključuje sistemsku particiju sa jezgrom operativnog sistema, bibliotekama, komponentama koje su neophodne za pokretanje uređaja i standardnim aplikacijama koje dolaze sa uređajem (npr. aplikacije za telefon, poruke, kalendar).

1. /data:

Ovde se nalaze podaci korisnika i instalirane aplikacije. Svaka aplikacija ima svoj direktorijum unutar /data particije gde čuva svoje podatke, postavke i bazu podataka. Takođe, ovo je mesto gde se čuvaju privremeni podaci.

1. /cache:

Ovaj direktorijum sadrži privremene fajlove koje generišu aplikacije ili sistem. Ovi fajlovi su često privremeno smešteni ovde kako bi se ubrzao pristup ili omogućio brži rad aplikacija.

1. /sdcard ili /storage:

Ovo je mesto gde se čuvaju korisnički podaci, kao što su slike, video zapisi, muzika i preuzete datoteke. Može biti fizička SD kartica ili interna memorija uređaja, u zavisnosti od konfiguracije uređaja.

1. /system/vendor:

Ovaj direktorijum sadrži datoteke i resurse koje je proizvođač uređaja dodao na uređaj. To može uključivati drajvere za hardver, dodatne aplikacije i druge sistemske resurse.

1. /system/app i /data/app:

Ovi direktorijumi sadrže instalirane aplikacije na uređaju. /system/app sadrži aplikacije koje su deo osnovne instalacije operativnog sistema, dok /data/app sadrži aplikacije koje su preuzete ili instalirane od strane korisnika.

1. /proc i /sys:

Ovi direktorijumi pružaju informacije o trenutnom stanju sistema i omogućavaju pristup parametrima i konfiguracijama kernela i sistema.

8. /recovery:

Ova particija sadrži sistem za vraćanje (recovery system), koji se koristi za vraćanje uređaja u fabričko stanje, instaliranje zakrpa (patches) i ažuriranja, kao i za rešavanje problema sa uređajem.

Ovo su samo neki od ključnih direktorijuma u Android datotečnom sistemu. Razumevanje strukture datotečnog sistema može biti korisno prilikom razvoja aplikacija, kao i za forenzička istraživanja i analizu mobilnih uređaja.

# Metodologija digitalne forenzike

Metodologija digitalne forenzike je sistematičan pristup istraživanju digitalnih uređaja, podataka i sistema radi prikupljanja, analize i interpretacije digitalnih dokaza. Kada je reč o Android mobilnim uređajima, primena metodologije digitalne forenzike zahteva posebno prilagođene principe i postupke.

Digitalna forenzika, posebno kada se primenjuje na Android mobilne uređaje, zasniva se na nizu osnovnih principa i postupaka koji omogućavaju prikupljanje, analizu i interpretaciju digitalnih dokaza. Ovi principi i postupci su ključni za obezbeđivanje integriteta dokaza, poverljivost informacija i validnost rezultata istraživanja. Opis osnovnih principa i postupaka digitalne forenzike primenjenih na Android mobilne uređaje:

1. **Zaštita integriteta podataka**: Centralni princip digitalne forenzike je očuvanje integriteta podataka. To znači da se tokom istraživanja mora voditi računa da se originalni podaci ne izmene ili oštete. Prilikom prikupljanja dokaza sa Android uređaja, potrebno je koristiti specijalizovane alate i tehnike koji omogućavaju kopiranje podataka bez njihove modifikacije.
2. **Pristup samo sa dozvolama**: Pristup Android uređajima i njihovim podacima se mora vršiti u skladu sa zakonskim propisima i etičkim smernicama. To podrazumeva da se pristup uređajima i podacima može ostvariti samo uz dozvolu vlasnika uređaja ili na osnovu sudskog naloga.
3. **Diskretnost i poverljivost**: Pri obavljanju forenzičkih istraživanja na Android uređajima, neophodno je obezbediti diskretnost i poverljivost informacija. To znači da se prilikom rukovanja podacima mora voditi računa o zaštiti privatnosti korisnika i o sprečavanju neovlašćenog pristupa informacijama.
4. **Dokumentacija i evidencija**: Svi koraci u procesu forenzičke analize moraju biti dokumentovani i evidentirani. To uključuje dokumentovanje svih aktivnosti, alata koji su korišćeni, rezultata analize i zaključaka koji su izvučeni. Ova dokumentacija je ključna kako bi se osigurala verodostojnost rezultata istraživanja i kako bi se pružili dokazi koji su validni u pravnom kontekstu.
5. **Specijalizovani alati i tehnike**: Prilikom obavljanja forenzičkih analiza na Android uređajima, koriste se specijalizovani alati i tehnike koji omogućavaju efikasno prikupljanje, analizu i interpretaciju digitalnih dokaza. Ovi alati se često prilagođavaju specifičnim karakteristikama Android operativnog sistema i uređaja.

Ovi principi i postupci digitalne forenzike su ključni za obezbeđivanje validnih i pouzdanih rezultata istraživanja, posebno kada je reč o Android mobilnim uređajima koji sadrže veliku količinu osetljivih podataka i informacija. Poštovanje ovih principa omogućava stručnjacima za digitalnu forenziku da pruže relevantne dokaze i analize koje mogu biti od ključnog značaja u pravosudnim postupcima i istragama.

# 3.1. Opis forenzičkih koraka

Forenzički koraci prilikom analize Android uređaja obuhvataju niz detaljnih postupaka koji omogućavaju prikupljanje, analizu i interpretaciju digitalnih dokaza. Ovi koraci su ključni za obezbeđivanje integriteta i validnosti dokaza, kao i za pružanje relevantnih informacija koje mogu biti od značaja u istrazi ili pravnom postupku. Opis forenzičkih koraka:

A diagram of a collection

Description automatically generated

Slika 2. Tok procesa digitalne forenzike

1. Identifikacija:

* Prvi korak u forenzičkoj analizi Android uređaja je identifikacija ciljeva istraživanja. To uključuje razumevanje svrhe analize, definisanje obima istraživanja i identifikaciju relevantnih digitalnih artefakata.
* Identifikacija ciljeva može obuhvatiti utvrđivanje da li je cilj istraživanja vezan za određeni incident, kriminalnu aktivnost ili neki drugi događaj.

1. Sakupljanje:

* Nakon identifikacije ciljeva, sledeći korak je sakupljanje digitalnih dokaza sa Android uređaja. To uključuje kopiranje podataka sa različitih particija, poput /data, /system, /sdcard, kao i metapodataka o uređaju, instaliranih aplikacija, internet aktivnosti i drugih relevantnih informacija.
* Sakupljanje dokaza može se obaviti pomoću specijalizovanih alata za forenzičku analizu, kao što su UFED, Cellebrite, Oxygen Forensic Detective, kao i pomoću ADB alata za pristup Android uređaju putem komandne linije.

1. Analiza:

* Nakon sakupljanja dokaza, sledeći korak je detaljna analiza prikupljenih podataka. Ovo uključuje pregled fajlova, logova, baza podataka, poruka, slika, video zapisa, istorije pregleda i drugih digitalnih artefakata.
* Tokom analize, forenzički stručnjaci koriste specijalizovane alate i tehnike kako bi identifikovali relevantne informacije i tragove koji mogu biti od značaja za istraživanje.

1. Interpretacija:

* Poslednji korak u forenzičkoj analizi je interpretacija prikupljenih dokaza i izvođenje zaključaka. Ovo podrazumeva tumačenje pronađenih tragova i informacija kako bi se izvukli relevantni zaključci o događajima ili aktivnostima koji su se odvijali na Android uređaju.
* Interpretacija dokaza može uključivati rekonstrukciju događaja, identifikaciju potencijalnih zločinačkih aktivnosti, utvrđivanje odgovornosti ili pružanje podrške pravosudnim organima u donošenju informisanih odluka.

Ovi detaljni forenzički koraci su ključni za efikasnu analizu Android uređaja i pružanje relevantnih informacija koje mogu biti od ključnog značaja u istrazi ili pravnom postupku. Svaki korak se pažljivo izvodi uz poštovanje zakonskih i etičkih smernica kako bi rezultati analize bili validni i prihvatljivi u pravnom kontekstu.

# Alati i tehnike za forenzičku analizu Android uređaja

Alati i tehnike za forenzičku analizu Android uređaja obuhvataju širok spektar softverskih rešenja i metoda koje omogućavaju prikupljanje, analizu i interpretaciju digitalnih dokaza sa mobilnih uređaja koji koriste Android operativni sistem. Ovi alati su ključni za istražitelje i forenzičke stručnjake kako bi efikasno istražili i dokumentovali podatke sa Android uređaja, često kao deo kriminalističke istrage ili forenzičkog ispitivanja. Neki od popularnih alata i softverskih rešenja korišćenih za forenzičku analizu Android uređaja su:

1. Cellebrite UFED: Cellebrite UFED je jedan od vodećih komercijalnih alata za forenzičku analizu mobilnih uređaja, uključujući Android uređaje. Ovaj alat omogućava ekstrakciju podataka sa uređaja, analizu aplikacija, poruka, kontakata, istorije poziva i drugih digitalnih artefakata.
2. Oxygen Forensic Detective: Oxygen Forensic Detective je još jedan popularan komercijalni alat za forenzičku analizu Android uređaja. Ovaj alat omogućava detaljnu analizu podataka sa mobilnih uređaja, uključujući ekstrakciju podataka iz aplikacija, GPS lokacije, poruke, slike, video zapise i druge digitalne artefakte.
3. Autopsy: Autopsy je besplatan otvoreni izvor alat za forenzičku analizu digitalnih uređaja, uključujući Android mobilne uređaje. Ovaj alat omogućava analizu diskova, ekstrakciju podataka, pregled fajlova, metapodataka, poruka, lokacija i drugih digitalnih artefakata.
4. XRY: XRY je komercijalni alat za forenzičku analizu mobilnih uređaja koji podržava analizu Android uređaja. Ovaj alat omogućava ekstrakciju podataka sa uređaja, dekodiranje aplikacija, analizu komunikacionih podataka i rekonstrukciju događaja.
5. ADB (Android Debug Bridge): ADB je zvanični alat koji dolazi uz Android SDK i omogućava komunikaciju sa Android uređajima putem komandne linije. ADB se često koristi u forenzičkim analizama za pristupanje uređaju, ekstrakciju podataka i izvođenje različitih komandi za analizu.

Ovi alati i softverska rešenja omogućavaju forenzičkim istražiteljima da efikasno prikupe, analiziraju i interpretiraju digitalne dokaze sa Android mobilnih uređaja. Kombinacija ovih alata i tehnika omogućava detaljnu forenzičku analizu koja može biti od ključnog značaja u istrazi i pravnom postupku.

Alati i tehnike za forenzičku analizu Android uređaja obuhvataju širok spektar funkcionalnosti koje omogućavaju ekstrakciju podataka, analizu datoteka, dekompilaciju aplikacija i druge korake neophodne za dubinsko istraživanje mobilnih uređaja. Opis korišćenja ovih alata i tehnika:

1. **Ekstrakcija podataka**: Alati kao što su Cellebrite UFED i Oxygen Forensic Detective omogućavaju ekstrakciju podataka sa Android uređaja. Ovaj proces uključuje povezivanje uređaja sa računarom putem USB kabla i korišćenje softvera za ekstrakciju podataka koji omogućava kopiranje fajlova, baza podataka, poruka, kontakata i drugih digitalnih artefakata sa uređaja na računar.
2. **Analiza datoteka**: Alati poput Autopsy omogućavaju detaljnu analizu datoteka sa Android uređaja. Ovo uključuje pregled fajlova, metapodataka, strukturu direktorijuma, kao i identifikaciju skrivenih ili obrisanih fajlova koji mogu biti od forenzičkog značaja.
3. **Dekompilacija aplikacija**: Za analizu aplikacija na Android uređajima koriste se alati za dekompilaciju, poput jadx ili apktool. Ovi alati omogućavaju dekompilaciju APK datoteka aplikacija kako bi se proučili izvorni kodovi, resursi, manifesti i druge komponente aplikacije.
4. **Analiza baza podataka**: Forenzički stručnjaci koriste alate poput SQLite Browser ili DB Browser for SQLite za analizu baza podataka sa Android uređaja. Ovi alati omogućavaju pregled i analizu podataka u SQLite formatu, koji se često koristi za čuvanje informacija u Android aplikacijama.
5. **Analiza internet aktivnosti**: Alati poput Wireshark-a se koriste za analizu internet aktivnosti sa Android uređaja. Ovaj alat omogućava snimanje i analizu mrežnog saobraćaja, identifikaciju posećenih web stranica, komunikaciju sa serverima, razmenu podataka i druge aktivnosti koje mogu biti od forenzičkog interesa.
6. **Analiza lokacijskih podataka**: Forenzički istražitelji mogu koristiti alate kao što su Google Location History ili GPS Logger za analizu lokacijskih podataka sa Android uređaja. Ovi alati omogućavaju pregled lokacijskih istorija, geotagova slika, GPS tragova i drugih podataka koji mogu biti relevantni za istraživanje.

Korišćenje ovih alata i tehnika omogućava forenzičkim istražiteljima da dubinski istraže Android uređaje i izvuku relevantne informacije koje mogu biti od ključnog značaja u kriminalističkim istragama, sudskim procesima ili drugim pravnim postupcima. Svaki korak se pažljivo izvodi uz poštovanje zakonskih i etičkih smernica kako bi rezultati bili validni i prihvatljivi u pravnom kontekstu.

# Forenzička analiza mobilnih aplikacija

Forenzička analiza mobilnih aplikacija, posebno na Android platformi, zahteva upotrebu specifičnih metoda i tehnika kako bi se istražila i dokumentovala aktivnost aplikacija, kao i potencijalno prisutni digitalni dokazi. Neke od ključnih metoda i tehnika korišćenih za analizu Android aplikaciju su:

* **Statička analiza**: Ova metoda podrazumeva analizu aplikacije bez njene izvršne aktivnosti. Forenzički stručnjaci mogu koristiti alate poput jadx, apktool, ili dex2jar kako bi dekompilirali APK datoteku aplikacije i analizirali izvorni kod, resurse, manifest fajlove i druge komponente. Ova analiza može otkriti potencijalne ranjivosti, skrivene funkcije, sporne permisije i druge sumnjive aktivnosti.
* **Dinamička analiza**: Ova metoda uključuje izvršavanje aplikacije u kontrolisanom okruženju radi praćenja njenog ponašanja u realnom vremenu. Forenzički stručnjaci mogu koristiti alate kao što su Android Debug Bridge (ADB) ili emulatore kako bi pokrenuli aplikaciju i pratili njenu interakciju sa sistemom. Ovo može pomoći u otkrivanju sumnjivih mrežnih zahteva, aktivnosti skladištenja podataka, interakcija sa sistemskim resursima i drugih potencijalno spornih radnji.
* **Analiza mrežne komunikacije**: Ova tehnika podrazumeva praćenje i analizu mrežnih zahteva i odgovora koje aplikacija šalje i prima tokom svog izvršavanja. Alati poput Wireshark-a mogu se koristiti za snimanje mrežnog saobraćaja i analizu HTTP, HTTPS, TCP/IP, DNS i drugih protokola koji se koriste u komunikaciji. Ovo može pomoći u otkrivanju neovlašćenog slanja ili primanja podataka, kao i komunikacije sa sumnjivim serverima.
* **Analiza baze podataka**: Mnoge aplikacije koriste lokalne baze podataka za skladištenje podataka kao što su korisnički podaci, postavke, istorija aktivnosti i druge informacije. Forenzički stručnjaci mogu koristiti alate poput SQLite Browser-a ili adb alata za pristupanje bazi podataka aplikacije i analizu njenog sadržaja. Ovo može pomoći u identifikaciji osetljivih informacija, kao i u rekonstrukciji korisničkih aktivnosti.
* **Analiza aplikacionih fajlova**: Ova tehnika uključuje analizu svih fajlova koji su deo instalacije aplikacije, uključujući ikone, slike, audio fajlove, XML fajlove i druge resurse. Forenzički stručnjaci mogu koristiti alate za dekompilaciju i analizu ovih fajlova kako bi identifikovali skrivene informacije, štetne kodove ili druge sumnjive elemente.

Ove metode i tehnike su ključne za efikasnu forenzičku analizu Android aplikacija i otkrivanje potencijalno zlonamernih aktivnosti ili ranjivosti. Kombinacija statičke i dinamičke analize, praćenje mrežnog saobraćaja i analiza baza podataka omogućava detaljan uvid u aktivnosti aplikacija i pruža relevantne dokaze koji mogu biti od ključnog značaja u istrazi ili pravnom postupku.

# 5.1. Proces ekstrakcije korisnih informacija iz APK datoteka

Proces ekstrakcije korisnih informacija iz APK (Android Package) datoteka je ključni korak u forenzičkoj analizi mobilnih aplikacija. APK datoteke su arhive koje sadrže sve komponente jedne Android aplikacije, uključujući izvorni kod, resurse, manifest fajlove i druge metapodatke. Ekstrakcija korisnih informacija iz APK datoteka omogućava forenzičkim istražiteljima pristup detaljima o aplikaciji koji su od značaja za analizu i istraživanje. Proces ekstrakcije korisnih informacija:

A diagram of a software application

Description automatically generated

Slika 3. APK struktura

* **Dekompilacija APK datoteke**: Prvi korak u procesu ekstrakcije je dekompilacija APK datoteke kako bi se dobili izvorni kod i resursi aplikacije. Postoje razni alati koji omogućavaju dekompilaciju APK datoteka, kao što su jadx, apktool, dex2jar i druge slične aplikacije. Ovi alati dekompiliraju APK datoteku i omogućavaju pristup izvornom kodu aplikacije, resursima kao što su slike, ikone, XML fajlovi, manifest fajl i druge komponente.
* **Analiza manifest fajla**: Manifest fajl je XML fajl koji sadrži osnovne informacije o aplikaciji, uključujući naziv paketa, verziju, dozvole (permissions), aktivnosti, servise, prijemnike i druge komponente. Forenzički istražitelji analiziraju manifest fajl kako bi identifikovali dozvole koje aplikacija zahteva, potencijalne sigurnosne ranjivosti ili zlonamerne aktivnosti.
* **Pregled izvornog koda aplikacije**: Dekompilacija APK datoteke omogućava pristup izvornom kodu aplikacije, koji se obično nalazi u Java ili Kotlin programskom jeziku. Forenzički istražitelji pregledaju izvorni kod kako bi identifikovali potencijalne sigurnosne ranjivosti, skrivene funkcije, kodne zapise povezane sa štetnim aktivnostima ili druge sumnjive elemente.
* **Analiza resursa**: Resursi aplikacije, kao što su slike, ikone, audio fajlovi, XML fajlovi za postavke i druge komponente, takođe se mogu ekstrahovati iz APK datoteke i analizirati. Ovo može pomoći u identifikaciji skrivenih poruka, slika ili informacija koje mogu biti od značaja za forenzičku analizu.
* **Pronalaženje skrivenih datoteka ili informacija**: Ponekad aplikacije mogu sadržavati skrivene datoteke ili informacije koje nisu lako vidljive prilikom standardne upotrebe. Forenzički istražitelji mogu koristiti alate za analizu datoteka kako bi pregledali sadržaj aplikacije i identifikovali potencijalno skrivene ili štetne elemente.

Proces ekstrakcije korisnih informacija iz APK datoteka omogućava forenzičkim istražiteljima detaljnu analizu aplikacija, identifikaciju potencijalnih sigurnosnih ranjivosti, skrivenih funkcija ili štetnih aktivnosti koje mogu biti od značaja za istraživanje ili pravni postupak. Ova analiza pruža relevantne informacije koje mogu biti ključne u otkrivanju zlonamernih aktivnosti ili dokazivanju odgovornosti.

# Analiza podataka i korisničkih informacija

Analiza podataka i korisničkih informacija na Android uređajima zahteva primenu različitih forenzičkih tehnika kako bi se identifikovali, prikupili i interpretirali relevantni digitalni dokazi. Ovaj proces obuhvata različite vrste podataka kao što su kontakti, SMS poruke, istorija poziva, slike i druge informacije koje su od značaja za istražitelje i forenzičke stručnjake. Neke od ključnih tehnika korišćenih u analizi podataka korisnika na Android uređajima su:

* Ekstrakcija podataka
* Analiza baza podataka
* Analiza fajlova sistema
* Analiza mrežne aktivnosti
* Analiza meta podataka

1. Ekstrakcija podataka

Ekstrakcija podataka sa Android uređaja je ključni korak u digitalnoj forenzici, omogućavajući forenzičarima pristup podacima sa uređaja radi analize i prikupljanja dokaza. Neke od metoda za ekstrakciju su:

A green and white text on a green and white background

Description automatically generated with medium confidence

Slika 4. Metode za ekstrakciju podataka sa Android uređaja

* **Ručna ekstrakcija**: Ispitivač koristi korisnički interfejs mobilnog uređaja za istraživanje sadržaja. Dok pregleda uređaj, ispitivač pravi fotografije svakog ekrana. Ovaj metod ne zahteva upotrebu alata za izvršenje ekstrakcije podataka. Pored prednosti, najveći nedostatak ovog metoda je taj što se može povratiti samo vidljivi podaci korisnicima na telefonu, i očigledno da je vremenski zahtevan.
* **Fizička ekstrakcija**: Fizička ekstrakcija podataka obuhvata direktno kopiranje sadržaja memorije uređaja, uključujući operativni sistem, aplikacije i korisničke podatke. To se obično radi korišćenjem specijalizovanih alata koji pristupaju memoriji uređaja putem USB konekcije ili drugih fizičkih interfejsa. Ova metoda omogućava dublju analizu podataka, uključujući izbrisane ili skrivene informacije. Međutim, fizička ekstrakcija nije uvek moguća na svim uređajima i može zahtevati posebne veštine i alate.
* **Logička ekstrakcija**: Logička ekstrakcija podataka se fokusira na izvlačenje korisničkih podataka putem softverskih interfejsa koji su dostupni na uređaju. To može uključivati korišćenje alata poput Android Debug Bridge (ADB) ili specijalizovanih softvera za forenzičku analizu. Ova metoda je manje invazivna od fizičke ekstrakcije, ali može pružiti korisne informacije poput kontakata, poruka, istorije poziva i drugih podataka sa uređaja.

Koristeći ove tehnike ekstrakcije podataka, forenzičari mogu pristupiti različitim tipovima informacija sa Android uređaja i koristiti ih u istrazi ili pravnom procesu. Važno je napomenuti da postupci ekstrakcije podataka moraju biti pažljivo sprovedeni kako bi se osigurala integritet i admissibility prikupljenih dokaza.

1. Analiza baza podataka

Analiza baza podataka na Android uređajima predstavlja važan korak u forenzičkoj analizi, omogućavajući istražiteljima pristup različitim korisničkim informacijama koje se čuvaju unutar aplikacija. Sledi detaljniji opis ovog procesa:

* **Identifikacija relevantnih baza podataka**: Prvi korak u analizi baza podataka je identifikacija relevantnih baza koje sadrže korisničke informacije od interesa. To može uključivati baze podataka aplikacija za poruke, kontakte, istoriju poziva, postavke aplikacija, kao i druge podatke koji se često čuvaju lokalno na uređaju.
* **Ekstrakcija baza podataka**: Nakon identifikacije relevantnih baza podataka, forenzičari koriste odgovarajuće alate i tehnike za ekstrakciju baza podataka sa Android uređaja. Ovo može uključivati korišćenje softverskih alata za forenzičku ekstrakciju, kao i ručno pretraživanje datoteka sistema radi pronalaženja baza podataka.
* **Analiza strukture baza podataka**: Nakon ekstrakcije, forenzičari analiziraju strukturu baza podataka kako bi razumeli organizaciju podataka unutar njih. Ovo obično uključuje pregled šema baze podataka, tabela, ključeva i veza između različitih entiteta.
* **Izvlačenje korisnih informacija**: Nakon analize strukture baza podataka, forenzičari izvlače korisne informacije koje su od interesa za istraživanje. Ovo može uključivati kontakt informacije, SMS poruke, istoriju poziva, postavke aplikacija, lozinke, slike, audio zapise i druge podatke koji su relevantni za slučaj.
* **Analiza podataka**: Konačno, forenzičari analiziraju izvučene podatke kako bi identifikovali ključne informacije, potencijalne dokaze ili sumnjive aktivnosti. Ova analiza može uključivati pregled teksta poruka, identifikaciju kontakata, rekonstrukciju istorije poziva, identifikaciju poslatih ili primljenih medijskih datoteka i druge relevantne aktivnosti.

Analiza baza podataka pruža dublji uvid u korisničke informacije na Android uređajima i omogućava forenzičarima da identifikuju ključne dokaze koji mogu biti od koristi u istrazi ili pravnom procesu. Važno je voditi računa o integritetu i autentičnosti prikupljenih podataka kako bi se osigurala validnost forenzičkih dokaza.

1. Analiza fajlova sistema

Analiza fajlova sistema predstavlja važan deo forenzičke analize Android uređaja, omogućavajući forenzičarima da pristupe i analiziraju različite fajlove i direktorijume na uređaju. Sledi detaljniji opis ovog procesa:

* **Pregled direktorijuma**: Forenzička analiza počinje pregledom različitih direktorijuma na Android uređaju. Ovo uključuje standardne direktorijume kao što su Download, Pictures, Documents, DCIM, i druge lokacije gde se često čuvaju korisnički podaci.
* **Identifikacija korisničkih podataka**: Nakon pregleda direktorijuma, forenzičari identifikuju i pregledaju fajlove koji mogu sadržavati korisničke podatke od interesa. Ovo mogu biti slike, video zapisi, dokumenti, zvučni zapisi, preuzete datoteke sa interneta i druge vrste fajlova.
* **Analiza meta podataka**: Uz pregled samih fajlova, forenzičari analiziraju i meta podatke koji se često čuvaju uz fajlove. Ovi meta podaci mogu sadržavati informacije o vremenu kreiranja ili modifikacije fajlova, lokaciji, informacijama o autoru ili uređaju sa kog je fajl kreiran, i druge relevantne informacije.
* **Izvlačenje dokaza**: Na osnovu analize fajlova sistema, forenzičari izvlače korisne informacije ili dokaze koji mogu biti od značaja za istraživanje. Ovo može uključivati identifikaciju važnih slika ili dokumenata, rekonstrukciju vremenske linije događaja, ili identifikaciju tragova aktivnosti korisnika na uređaju.
* **Identifikacija sumnjivih ili skrivenih fajlova**: Pored standardnih korisničkih podataka, forenzičari takođe traže sumnjive ili skrivene fajlove koji mogu ukazivati na nezakonite aktivnosti ili pokušaje skrivanja informacija. Ovo uključuje pregled sistema fajlova i detekciju potencijalno sumnjivih fajlova ili direktorijuma.

Analiza fajlova sistema omogućava forenzičarima da identifikuju korisničke podatke, tragove aktivnosti i potencijalne dokaze na Android uređajima, što može biti od ključnog značaja u istrazi ili pravnom procesu. Važno je voditi računa o integritetu i autentičnosti prikupljenih dokaza kako bi se osigurala validnost forenzičkih nalaza.

1. Analiza mrežne aktivnosti

Analiza mrežne aktivnosti predstavlja ključni deo forenzičke analize Android uređaja, omogućavajući istražiteljima da prate komunikaciju uređaja sa spoljnim serverima i identifikuju eventualne sumnjive ili nezakonite aktivnosti. Sledi detaljniji opis ovog procesa:

* **Praćenje mrežne komunikacije**: Forenzičari prate mrežnu komunikaciju Android uređaja kako bi identifikovali sve odlazne i dolazne veze sa spoljnim serverima. Ovo uključuje praćenje HTTP/HTTPS zahteva i odgovora, DNS upita, TCP/IP veza i drugih oblika komunikacije.
* **Analiza mrežnih logova**: Pregled mrežnih logova omogućava forenzičarima da detaljno analiziraju svaki aspekt mrežne komunikacije. To uključuje informacije kao što su IP adrese, vremenski žigovi, vrste zahteva i odgovora, URL adrese, paketne informacije i druge relevantne detalje.
* **Identifikacija sumnjivih aktivnosti**: Na osnovu analize mrežne komunikacije, forenzičari traže sumnjive ili neobične aktivnosti koje bi mogle ukazivati na nezakonite radnje ili bezbednosne pretnje. Ovo može uključivati slanje ili primanje osetljivih podataka, pokušaje pristupa nepoznatim serverima, upotrebu neobičnih portova ili protokola, i druge sumnjive aktivnosti.
* **Korišćenje alata za analizu mrežnog saobraćaja**: Forenzičari često koriste specijalizovane alate poput Wireshark-a za detaljnu analizu mrežnog saobraćaja. Ovi alati omogućavaju prikupljanje, filtriranje i analizu mrežnih paketa, što olakšava identifikaciju sumnjivih aktivnosti i prikupljanje dokaza.
* **Dokumentovanje nalaza**: Konačno, forenzičari dokumentuju sve relevantne nalaze i dokaze otkrivene tokom analize mrežne aktivnosti. To uključuje detaljno opisivanje sumnjivih aktivnosti, beleženje IP adresa, URL adresa i drugih relevantnih informacija, kao i čuvanje dokaza radi dalje analize ili korišćenja u pravnom procesu.

Analiza mrežne aktivnosti omogućava forenzičarima da identifikuju potencijalne pretnje, prikupe dokaze o nezakonitim radnjama i pruže ključne informacije koje mogu biti od koristi u istrazi ili pravnom procesu. Važno je voditi računa o integritetu i autentičnosti prikupljenih dokaza kako bi se osigurala validnost forenzičkih nalaza.

1. Analiza meta podataka

Analiza meta podataka predstavlja važan deo forenzičke analize Android uređaja, omogućavajući forenzičarima da prikupe i analiziraju različite informacije koje prate aktivnosti korisnika. Sledi detaljniji opis ovog procesa:

* **Prikupljanje meta podataka**: Meta podaci su informacije koje prate druge podatke, pružajući dodatne kontekstualne informacije o njima. U kontekstu Android uređaja, meta podaci mogu uključivati informacije kao što su vreme slanja poruka, dužina poziva, geografske lokacije, vrsta i model uređaja, verzija operativnog sistema, informacije o mreži i drugi detalji.
* **Analiza vremenskih podataka**: Vreme slanja poruka, trajanje poziva i drugi vremenski podaci pružaju forenzičarima uvid u aktivnosti korisnika tokom određenog vremenskog perioda. Ovi podaci mogu biti ključni za rekonstrukciju vremenske linije događaja, identifikaciju uzoraka ponašanja ili utvrđivanje aktivnosti koje su se odvijale u određenom trenutku.
* **Analiza geografskih lokacija**: Informacije o geografskim lokacijama omogućavaju forenzičarima da prate kretanje korisnika i identifikuju mesta gde su se nalazili u određenom vremenskom periodu. Ovi podaci mogu biti korisni u istrazi zločina ili u identifikaciji lokacija gde su se odvijale određene aktivnosti.
* **Rekonstrukcija vremenske linije događaja**: Analiza meta podataka omogućava forenzičarima da rekonstruišu vremensku liniju događaja, prateći aktivnosti korisnika tokom vremena. Ovo može biti od ključne važnosti u istrazi zločina ili u pružanju dokaza o određenim aktivnostima ili interakcijama.
* **Identifikacija uzoraka ponašanja**: Na osnovu analize meta podataka, forenzičari mogu identifikovati uzorke ponašanja korisnika, što može pružiti uvid u navike, rutine ili aktivnosti koje su redovno izvodili. Ovo može biti korisno u analizi ponašanja korisnika ili identifikaciji neobičnih ili sumnjivih aktivnosti.

Analiza meta podataka omogućava forenzičarima da stvore kompletniju sliku o aktivnostima korisnika, što može biti od ključnog značaja u istrazi zločina ili pravnom procesu. Važno je voditi računa o integritetu i autentičnosti prikupljenih meta podataka kako bi se osigurala validnost forenzičkih nalaza.

# Android Debug Bridge (ADB)

ADB (Android Debug Bridge) je alat koji omogućava komunikaciju između računara i Android uređaja putem USB veze ili bežične mreže. To je važan deo Android razvojnog okruženja i pruža različite funkcionalnosti za razvoj aplikacija, testiranje, debagiranje i forenzičku analizu Android uređaja.

A green robot with a blackboard and white text

Description automatically generated

Slika 5. ADB (Android Debug Bridge) alat

Značaj ADB alata u Android razvoju i analizi može se sagledati kroz nekoliko ključnih tačaka:

1. **Pristup terminalu uređaja**: ADB omogućava pristup terminalu Android uređaja direktno sa računara. To omogućava izvršavanje raznih komandi i operacija na uređaju, što je korisno za dijagnostiku, debagiranje i izvođenje različitih operacija.
2. **Instalacija i deinstalacija aplikacija**: Razvojni programeri koriste ADB za instalaciju, deinstalaciju i upravljanje aplikacijama na Android uređajima. To je ključno za razvoj i testiranje aplikacija na stvarnim uređajima.
3. **Kopiranje datoteka**: ADB omogućava kopiranje datoteka između računara i Android uređaja. To je korisno za prenos fajlova kao što su aplikacije, medijski sadržaj ili forenzički alati.
4. **Debagovanje aplikacija**: Razvojni programeri koriste ADB za debagiranje aplikacija instaliranih na uređaju. To uključuje prikupljanje debug informacija, praćenje logova i testiranje performansi aplikacija.
5. **Forenzička analiza**: ADB se takođe koristi u forenzičkoj analizi Android uređaja. Omogućava prikupljanje podataka, ekstrakciju logova i drugih forenzičkih aktivnosti koje su ključne za istražitelje i forenzičare.

ADB alat je ključni deo Android razvojnog okruženja i pruža različite mogućnosti za rad sa Android uređajima. Bez njega, razvoj aplikacija, testiranje, debagiranje i forenzička analiza Android uređaja bili bi značajno otežani.

**Kako pokrenuti ADB alat na računaru?**

Pokretanje ADB alata na računaru je relativno jednostavan proces. Korake koje treba preduzeti su:

1. **Instalacija Android SDK-a (Software Development Kit)**: Prvi korak je instalacija Android SDK-a na računar. Android SDK sadrži ADB alat, zajedno sa ostalim alatima i resursima koji su potrebni za razvoj Android aplikacija. Može se preuzeti Android SDK sa zvanične Android developerske stranice.
2. **Podešavanje putanje (opciono)**: Nakon instalacije Android SDK-a, može da se podesi putanja (PATH) kako bi računar mogao prepoznati ADB alat kada se poziva iz komandne linije. Ovo se obično radi dodavanjem putanje do direktorijuma koji sadrži ADB alat u sistemsku promenljivu PATH.
3. **Povezivanje Android uređaja sa računarom**: Da bi se mogao koristiti ADB alat, Android uređaj mora biti povezan sa računarom preko USB kabla ili bežične veze. Potrebno je proveriti da je USB debugiranje omogućeno na Android uređaju. Ova opcija se obično nalazi u podešavanjima uređaja pod opcijom "Developer Options".
4. **Pokretanje ADB alata**: Nakon što je uređaj povezan, može se pokrenuti ADB alat iz komandne linije. Potrebno je otvoriti terminal ili Command Prompt na računaru i uneti komandu za pokretanje ADB-a. Na primer, ako je korišćena instalacija putem Android SDK-a, može se pokrenuti ADB komandom **adb**.
5. **Provera konekcije (opciono)**: Da bi se proverilo da li je uređaj uspešno povezan sa ADB-om, može se uneti komanda **adb devices** u komandnu liniju. Ova komanda će prikazati listu povezanih uređaja. Ako je uređaj uspešno prepoznat, trebalo bi da se pojavi na listi.

Nakon što se uspešno pokrene ADB alat i poveže uređaj, mogu se koristiti različite komande za upravljanje uređajem, instalaciju aplikacija, prenos datoteka, debagiranje i druge operacije.

**Kako povezati ADB sa Android uređajem?**

Povezivanje ADB (Android Debug Bridge) sa Android uređajem može se obaviti putem USB-a ili bežične mreže, u zavisnosti od potreba i postavki uređaja.

**Povezivanje preko USB-a:**

* Prvo, koristi se USB kabl koji dolazi sa Android uređajem i poveže se jedan kraj kabla sa USB portom na računaru.
* Zatim, poveže se drugi kraj kabla sa USB portom na Android uređaju.
* Na uređaju, ako nije već omogućeno, otvoriti "Developer Options" u podešavanjima uređaja i omogućiti "USB Debugging" opciju.
* Nakon što je USB Debugging omogućen, uređaj će biti prepoznat od strane ADB-a kada se pokrene na računaru.

**Povezivanje preko bežične mreže**:

* Ova opcija zahteva dodatne korake za podešavanje, ali omogućava bežičnu komunikaciju između računara i Android uređaja.
* Prvo, obezbediti da su računar i Android uređaj povezani na istu Wi-Fi mrežu.
* Na uređaju, otvoriti "Developer Options" i pronaći "Wireless Debugging" opciju. Omogućiti ovu opciju.
* Kada je Wireless Debugging omogućen, uređaj će prikazati IP adresu i port koji treba koristiti za bežičnu vezu.
* Na računaru, pokrenuti terminal ili Command Prompt i uneti komandu **adb connect <IP\_adresa\_uređaja>:<port>**. Umesto "<IP\_adresa\_uređaja>" i "<port>", uneti tačnu IP adresu i port koji je prikazan na uređaju.
* Nakon toga, uređaj će biti povezan sa ADB-om preko bežične mreže.

Nakon uspešnog povezivanja, mogu se koristiti ADB komande za upravljanje uređajem, instalaciju aplikacija, prenos datoteka, debagiranje i druge operacije, bez obzira na to da li je veza preko USB kabla ili bežična mreža.

**Osnovne komande i operacije koje se mogu izvršiti pomoću ADB alata**

ADB (Android Debug Bridge) alat omogućava različite komande i operacije za upravljanje Android uređajima putem računara. Neke od osnovnih komandi i operacija koje se mogu izvršiti pomoću ADB-a su:

**Povezivanje sa uređajem**:

* Komanda: **adb devices**
* Opis: Ova komanda prikazuje listu svih Android uređaja koji su trenutno povezani sa računarom putem ADB-a. ADB mora biti pokrenut na računaru kako bi se ova komanda uspešno izvršila.

**Prikaz informacija o uređaju**:

* Komanda: **adb shell getprop**
* Opis: Ova komanda prikazuje osnovne informacije o uređaju kao što su model, serijski broj, verzija Android operativnog sistema i druge sistemski properti.

**Instalacija aplikacija**:

* Komanda: **adb install <putanja\_do\_aplikacije.apk>**
* Opis: Ova komanda instalira Android aplikaciju na povezani uređaj. "<putanja\_do\_aplikacije.apk>" treba zameniti stvarnom putanjom do APK datoteke koju želite da instalirate.

**Deinstalacija aplikacija**:

* Komanda: **adb uninstall <ime\_paketa>**
* Opis: Ova komanda deinstalira Android aplikaciju sa uređaja. "<ime\_paketa>" treba zameniti identifikatorom paketa aplikacije koju želite da deinstalirate.

**Kopiranje datoteka između računara i uređaja**:

* Komanda: **adb push <lokalna\_datoteka> <udaljena\_lokacija\_na\_uređaju>**
* Opis: Ova komanda kopira datoteku sa računara na određenu lokaciju na Android uređaju.

**Prenošenje datoteka sa uređaja na računar**:

* Komanda: **adb pull <udaljena\_datoteka\_na\_uređaju> <lokalna\_lokacija\_na\_računaru>**
* Opis: Ova komanda prenosi datoteku sa određene lokacije na Android uređaju na računar.

**Pristup terminalu uređaja**:

* Komanda: **adb shell**
* Opis: Ova komanda otvara interaktivnu komandnu liniju (shell) na povezanom Android uređaju, što omogućava izvršavanje različitih sistemskih komandi i skripti direktno na uređaju.

**Eksport SMS poruka**:

* Komanda: **adb shell content query --uri content://sms/**
* Ova komanda izlistava sve SMS poruke sa uređaja. Možete koristiti redirect operator > da biste preusmerili rezultate u datoteku ako želite da ih sačuvate: adb shell content query --uri content://sms/ > sms.txt

**Eksport istorije poziva**:

* Komanda: **adb shell content query --uri content://call\_log/calls**
* Ova komanda izlistava istoriju poziva sa uređaja. Takođe, možete preusmeriti rezultate u datoteku: adb shell content query --uri content://call\_log/calls > call\_log.txt

**Eksport kontakata**:

* Komanda: **adb shell content query --uri content://contacts/phones**
* Ova komanda izlistava kontakte sa uređaja. Rezultate možete preusmeriti u datoteku: adb shell content query --uri content://contacts/phones > contacts.txt

**Pravljenje screenshot-a**:

* Komanda: **adb exec-out screencap -p > screenshot.png**
* Ova komanda pravi screenshot trenutnog ekrana uređaja i čuva ga kao sliku pod nazivom "screenshot.png" u radnom direktorijumu na računaru.

Ove su samo neke od osnovnih komandi koje se mogu koristiti sa ADB-om. Postoje i mnoge druge komande i operacije koje omogućava ADB alat, uključujući debagiranje, snimanje ekrana, pristup logovima sistema, i mnoge druge.

**Sigurnosni aspekti i predostrožnosti**

Korišćenje ADB (Android Debug Bridge) alata može predstavljati određene sigurnosne rizike, posebno kada se koristi u kontekstu forenzičke analize ili pristupa osetljivim podacima. Evo nekoliko sigurnosnih aspekata i predostrožnosti koje treba uzeti u obzir:

**Sigurnosni rizici**:

* Neovlašćeni pristup: ADB alat omogućava pristup uređaju preko USB-a ili bežične mreže, što može dovesti do neovlašćenog pristupa uređaju i podacima.
* Mogućnost zloupotrebe: Korišćenje ADB-a može omogućiti zlonamernim korisnicima da izvrše različite vrste napada, kao što su preuzimanje osetljivih podataka, instalacija malvera ili promena postavki uređaja.
* Potencijalne sigurnosne ranjivosti: ADB alat sam po sebi može imati sigurnosne ranjivosti koje mogu biti iskorišćene za napade na uređaje.

**Mere opreza**:

* Omogućavanje USB Debugging-a samo kada je potrebno: Korisnici bi trebalo da omoguće USB Debugging samo kada je neophodno za razvoj ili analizu, a zatim ga isključe kada nije potreban kako bi se smanjio rizik od neovlašćenog pristupa.
* Ograničavanje pristupa: Ako je moguće, trebalo bi ograničiti pristup ADB alatu na pouzdane računare ili mreže kako bi se smanjio rizik od neovlašćenog pristupa.
* Redovno ažuriranje: Korisnici bi trebalo redovno da ažuriraju ADB alat kako bi se ispravile poznate sigurnosne ranjivosti i poboljšala sigurnost.

**Zaštita privatnosti i sigurnosti podataka**:

* Korišćenje sigurnih veza: Ako je moguće, trebalo bi koristiti enkriptovane veze prilikom korišćenja ADB alata kako bi se zaštitili osetljivi podaci tokom prenosa.
* Enkripcija podataka: Ukoliko se izvršava ekstrakcija osetljivih podataka sa uređaja, trebalo bi razmotriti enkripciju ovih podataka kako bi se osigurala njihova sigurnost tokom skladištenja ili prenosa.
* Poštovanje zakonskih propisa: Prilikom korišćenja ADB alata u forenzičke svrhe, važno je poštovati relevantne zakone i propise koji se odnose na zaštitu privatnosti i obradu podataka.

Implementacija ovih sigurnosnih mera i predostrožnosti pomaže u zaštiti privatnosti i sigurnosti podataka tokom korišćenja ADB alata za pristup uređajima i analizu podataka.

# Zaključak

Forenzika mobilnih uređaja, posebno Android platforme, postaje sve važnija kako tehnologija napreduje i kako se mobilni uređaji sve više koriste u svim aspektima života. Kroz ovaj rad, istražili smo osnove forenzičke analize Android uređaja, uključujući metode ekstrakcije podataka, analizu baza podataka, mrežne aktivnosti, meta podataka i druge relevantne tehnike. Takođe smo se upoznali sa alatima i tehnikama koji se koriste u ovom procesu.

Kroz analizu koraka forenzičke analize, shvatili smo značaj svakog koraka u otkrivanju i prikupljanju digitalnih dokaza, kao i važnost njihove pravilne interpretacije. Razumevanje strukture Android operativnog sistema, kao i metoda ekstrakcije podataka, omogućava forenzičarima da pronađu relevantne informacije koje mogu biti ključne u istrazi.

Uzimajući u obzir sve navedeno, možemo zaključiti da je forenzika Android mobilnih uređaja neophodan proces u savremenom digitalnom svetu. Kroz pravilno sprovedenu analizu, mogu se otkriti važni digitalni dokazi koji mogu poslužiti u istrazi krivičnih dela, zaštiti privatnosti korisnika, ili u drugim pravnim ili sigurnosnim kontekstima.

# Literatura

<https://fosonecy.home.blog/2021/05/15/database-and-file-system-structure-in-android-devices/>

<https://www.researchgate.net/figure/Digital-Forensics-Process-Flow_fig1_277076806>

<https://www.hackingloops.com/android-forensics-tutorial-part-3-data-acquisition-methods/>

<https://blog.salvationdata.com/2020/06/05/case-study-mobile-forensics-forensic-data-extraction-from-android-devices-using-adb-android-debug-bridge-part-ii/>