Univerzitet u Nišu,

Elektronski fakultet Niš



*Seminarski rad*

Digitalna forenzika

**FORENZIKA ANDROID MOBILNIH UREĐAJA**

Mentor: Student:

Prof. dr Bratislav Predić Andrija Milosavljević 1481

Niš, februar 2023. godine

**Sadržaj**

[**1. Uvod** 3](#_Toc127102497)

[**2. Osnovne karakteristike mobilnih uređaja** 4](#_Toc127102498)

[**3. Android operativni sistem** 6](#_Toc127102499)

[**3.1. Hijerarhija datoteka i struktura fajl sistema** 8](#_Toc127102500)

[**4. Forenzika mobilnih uređaja** 10](#_Toc127102501)

[**4.1. Izazovi mobilne forenzike** 12](#_Toc127102502)

[**4.2. Alati za forenziku mobilnih uređaja** 13](#_Toc127102503)

[**5. Metoda ekstrakcije** 16](#_Toc127102504)

[**5.1. Ručna ekstrakcija** 17](#_Toc127102505)

[**5.2. Logička ekstrakcija** 18](#_Toc127102506)

[**5.3. Fizička ekstrakcija** 18](#_Toc127102507)

[**5.4. Ostale metode ekstrakcije** 19](#_Toc127102508)

[**6. Android Debug Bridge (adb)** 20](#_Toc127102509)

[**7. Zaključak** 23](#_Toc127102510)

[**8. Literatura** 24](#_Toc127102511)

# **Uvod**

Mobilni uređaji su savremeni, višenamenski telekomunikacioni uređaji koji su postali nezaobilazni deo svakodnevnice pojedinca. Oni su široko prihvaćeni i lako dostupni krajnjim korisnicima što pokazuje i konstantan rast iz godine u godinu (*dijagram 1.*), a posebno je zanimljivo da svaki korisnik teži da savlada što veći broj funkcionalnosti, bez obzira na nivo obrazovanja [3]. Intenzivna upotreba u različitim sferama kao i njihova sposobnost memorisanja aktivnosti, pretvara ih u digitalne baze podataka. Samim tim, većina privatnih i poslovnih podataka se razmenjuje upravo preko mobilnih uređaja.

Mobilni uređaji se u osnovi sastoje iz standardnih komponenti kao što su: mikroprocesor, ROM (eng. Read Only Memory) memorija koja je nosilac operativnog sistema uređaja, RAM (eng. Random Access Memory) memorija koja se koristi za privremeno čuvanje podataka i omogućava procesoru da velikom brzinom pristupi podacima i da se u istom momentu koristi više aplikacija.

Mobilni uređaji mogu da čuvaju veliku količinu podataka kao što su:

* Telefonski pozivi – dolazni, odlazni, propušteni
* Poruke – SMS, MMS, Email, Instant messaging
* Fotografije i video zapisi – geotagovani
* Istorija Web pretraživača
* Beleške
* Ostale multimedijalne datoteke

Karakteristike i osobine samih uređaja postaju zanimljive kao nosioci informacija kako bezbednosnim strukturama radi prikupljanja dokaza, tako i kompanijama koje se bave izučavanjem sigurnosti podataka i sigurnosnim sistemima. Mobilni uređaji predstavljaju dobar izvor dokaza i informacija sa stanovišta digitalnog dokaza. Prema međunarodnoj definiciji u oblasti forenzičkih nauka, digitalni dokaz je svaka informacija u digitalnom obliku koja ima dokazujuću vrednost, i koja je ili uskladištena ili prenesena u takvom obliku. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i generisane dokazne informacije, digitalizovane audio i video dokazne signale, signale sa digitalnog mobilnog telefona, informacije sa digitalnih fax mašina i signale drugih digitalnih uređaja. Dakle, digitalni dokaz je bilo koja informacija generisana, obrađivana, skladištena ili prenesena u digitalnom obliku na koju se sud može osloniti kao na merodavnu.

Dijagram 1. Broj korisnika mobilnih uređaja (u milionima) od 2017-2022.

# **Osnovne karakteristike mobilnih uređaja**

Današnji pametni telefoni sastoje se iz dva elementarna dela: mobilnog uređaja i SIM (eng. Subscriber Identity Modules) kartice. Savremeni modeli telefona sadrže velike količine memorije i time imaju mogućnost čuvanja velike količine podataka.

Unutar samog uređaja moguće je pronaći sledeće informacije:

* ESN (eng. Electronic Serial Number) – jedinstveni serijski broj koji označava svaki uređaj
* MSISDN (eng. Mobile Subscriber Integrated Services Digital Network Number) – međunarodni pretplatnički broj
* IMEI (eng. International Mobile Equipment Identifier) – jedinstven generisani petnaestocifreni broj koji je dodeljen svakom mobilnom uređaju koji se koristi se za identifikaciju

Za uspostavljanje i pristup mobilnoj GSM mreži, neophodno je imati SIM karticu. Ona ima sličan sadržaj kao mobilni uređaj, sadrži jedinstvenu informaciju o korisniku, kodirane identifikacione podatke za mrežu, PIN (eng. Personal Identification Number) i ostale podatke poput telefonskog imenika, poruka, itd.

SIM kartica (*slika 2.1.*) je vrsta smart kartice koja ima mikroprocesor i memoriju (u opsegu između 8KB i 256KB) tipa EEPROM (eng. Electrically Erasable Programmable Read-Only Memory). U svojoj strukturi poseduje i radnu memoriju (RAM) koja se koristi prilikom izvršenja reprogramiranja memorije s operativnim sistemom i algoritmima za autorizaciju korisnika i enkripciju podataka. Glavnu ulogu ima mikroprocesor koji omogućava rad i sigurnost podataka. SIM kartica je zaštićena PIN brojem, čiji je zadatak ne samo zaštita podataka na kartici već i na samom uređaju. PIN broj je dugačak od četiri do osam cifara i vrši sigurnosnu opciju blokiranja uređaja ukoliko se unese pogrešan PIN određen broj puta – najčešće tri. Mobilni telefon se nakon blokiranja može otključati PUK brojem (eng. PIN Unblocking Key), a ako se kojim slučajem nekoliko puta unese i pogrešan PUK broj (najčešće 10 puta), uređaj se više ne može odblokirati.



Slika 2.1. Tipovi SIM kartica

Fajl sistem SIM kartice (*slika 2.2.*) je organizovan hijerarhijski na osnovu GSM 11.11. standarda. Sastoji se iz tri dela: Master File (MF) koji predstavlja koren fajl sistema, Dedicated File (DF) koji sadrži elementarne datoteke i Elementary File (EF) koje su u stvari datoteke.

Slika 2.2. Fajl sistem SIM kartice

Fajl sistem SIM kartice ima analogiju kao hijerarhija fajlova na hard disku i poseduje privilegije za upis, čitanje, brisanje i izmenu podatka. Veliki deo podataka može se čitati bez korišćenja PIN koda.

SIM kartica nam nudi nekoliko važnih informacija:

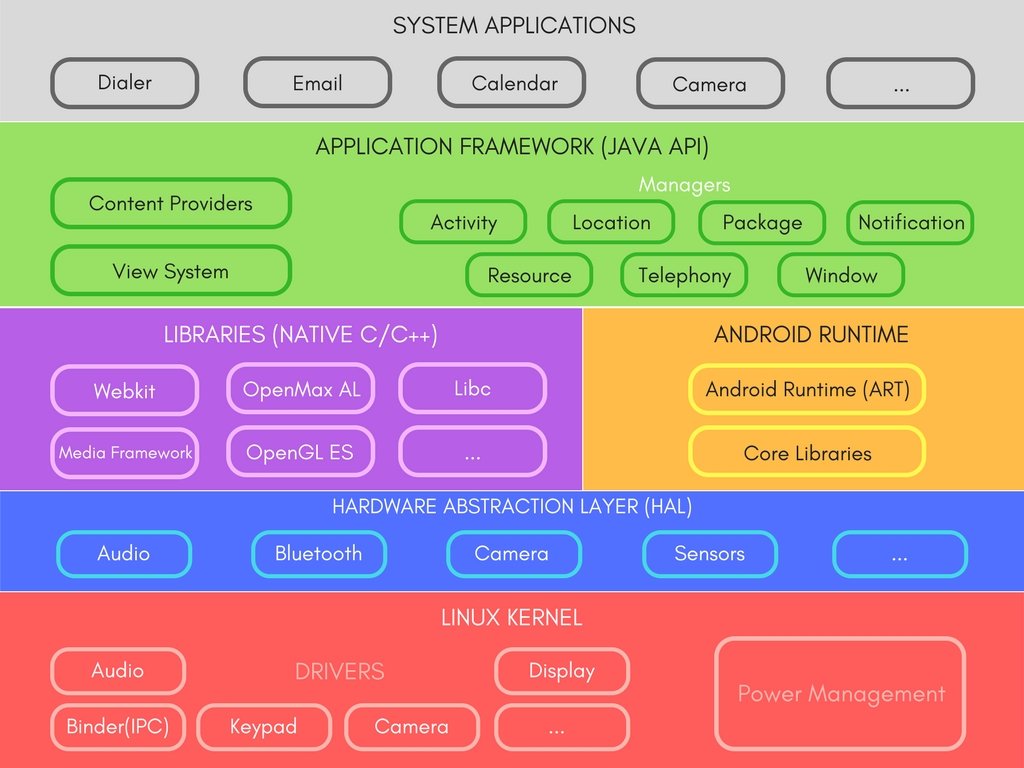
* ICCID (eng. Integrated Circuit Card Identifier) – međunarodni identifikator SIM kartice. Ovaj broj je fizički upisan na SIM kartici i ne može se menjati
* MSISDN (eng. Mobile Subscriber Integrated Services for Digital Network Number) – međunarodni pretplatnički broj
* IMSI (eng. International Mobile Subscriber Identity) – jedinstven identifikator SIM kartice: broj koji se sastoji od MCC (eng. Mobile Country Code), MNC (eng. Mobile Network Code) i MSIN (eng. Mobile Subscriber Identity Number)
* SPN (eng. Service Provider Name) – naziv mobilnog operatera

# **Android operativni sistem**

Android je operativni sistem zasnovan na Linux-u sa otvorenim kodom, koji je razvila kompanija Android Inc. 2003. godine. Google ga je otkupio 2005., a predstavio 2007. godine. S obzirom da je otvoren i besplatan, pogodan je za kompanije koje zahtevaju jeftin i fleksibilan operativni sistem za svoje pametne uređaje, bez razvoja novog operativnog sistema od nule. To je jedan od glavnih razloga njegovog širenja i popularnosti.

Android se bazira na jeziku Java i koristi virtualnu mašinu Dalvik za pokretanje aplikacija, pri čemu aplikacije dobijaju samo određeni deo sistemskih resursa, pa tako nemaju pristup delovima sistema koji su im nepotrebni, što donekle poboljšava sigurnost i stabilnost sistema, takođe pri instalaciji aplikacija korisnik dobija listu svih dozvola koje jedna aplikacija zahteva da bi se instalirala, što korisniku daje mogućnost da uoči potencijalno štetne aplikacije i obustavi njihovu instalaciju pre nego što dođe do oštećenja. Operativni sistem takođe sadrži skup biblioteka i komponenti za upravljanje uređajem, kao i aplikacije za sistemske usluge i korisnički interfejs.

Arhitektura Android operativnog sistema je kompleksna i sadrži mnoge različite komponente i slojeve koji su odgovorni za rad uređaja i pokretanje aplikacija što možemo videti na *slici 3.1*.



Slika 3.1. Arhitektura Android operativnog sistema

Android operativni sistem baziran je na Linux jezgru (engl. kernel) sa određenim promenama arhitekture koje je napravio Google. Linux je odabran jer se lako prilagođava različitim vrstama hardvera, što je neophodno da bi mogao funkcionisati na puno različitih vrsta uređaja. Linux jezgro je smešteno na dnu arhitekture i predstavlja sloj apstrakcije između hardvera uređaja i gornjih slojeva operativnog sistema.

Sloj hardverske apstrakcije (eng. Hardware Apstraction Layer - HAL) omogućava višem sloju (Java API Framework-u) rad sa hardverom mobilnih uređaja uz pomoć standardnih interfejsa. Ta funkcionalnost je moguća zahvaljujući bibliotekama koje pružaju interfejse za različite vrste hardverskih komponente, kao što su Bluetooth ili kamera.

Android Runtime – od verzije Android 5.0 svaka aplikacija se pokreće u vlastitom procesu i sa vlastitom instancom Android Runtime-a (ART) i omogućuje pokretanje više virtualnih računara sa malim memorijskim zahtevima izvršavanjem Dalvik Executable (DEX) datoteka.

Mnoge osnovne komponente i servisi Android sistema, uključujući i HAL i ART, programirane su u izvornom kodu, pa im je potrebna izvorna biblioteka napisana u programskim jezicima C i C++.

Java API Framework se koristi kako bi se olakšao razvoj aplikacija. Programeri mogu koristiti date interfejse da bi brzo i lako kreirali aplikacije koje koriste različite funkcionalnosti operativnog sistema. To omogućava programerima da se fokusiraju na razvoj korisničkog interfejsa i funkcionalnosti aplikacije, a ne na implementaciji osnovnih funkcionalnosti operativnog sistema.

Najviši sloj u Androidu sastoji se od aplikacija i sa njima korisnici komuniciraju. Postoje dve vrste aplikacija:

* Sistemske aplikacije – već su instalirane na mobilnom uređaju i isporučuju se sa istim. Tu spadaju aplikacije za upravljanje mrežom (WiFi, mobilna mreža), upravljanje procesima, upravljanje baterijom, ali i web pretraživači, aplikacije za elektronsku poštu, kontakti, aplikacija za telefonske razgovore i slično. Ove aplikacije se ne mogu deinstalirati ili menjati od strane korisnika, nego samo onemogućiti. Ove aplikacije nalaze se u */system* particiji.
* Korisničke aplikacije – instaliraju se sa Google Play prodavnice koja je službeni repozitorijum Android aplikacija.

Ova arhitektura omogućava operativnom sistemu da pruži širok spektar funkcionalnosti i da se prilagođava različitim vrstama hardvera i aplikacija. To takođe omogućava programerima da lako razvijaju aplikacije za ovaj operativni sistem koristeći Java API Framework i druge alate za razvoj [4].

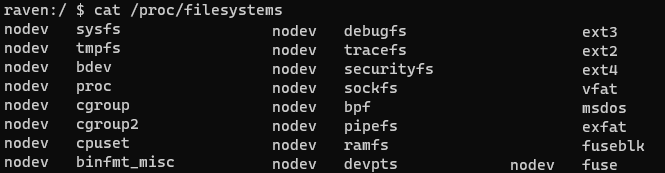
## **3.1. Hijerarhija datoteka i struktura fajl sistema**

Particije su način logičkog organizovanja podataka unutar memorije uređaja i omogućavaju logičku distribuciju prostora za skladištenje na delove kojima se može pristupiti nezavisno jedan od drugog. Izgled particija varira između dobavljača i verzija, ali postoji nekoliko particija na svim Android uređajima [2].

Ovo su najčešće Android particije koje se nalaze na većini uređaja:

* */boot* – kao što samo ime kaže, ova particija sadrži potrebne podatke i datoteke za pokretanje operativnog sistema mobilnog uređaja. Bez ove particije mobilni uređaj ne može pokrenuti procese
* */cache* – ova particija se koristi za skladištenje podataka kojima se često pristupa i razne druge datoteke poput logova za oporavak i paketa za ažuriranje
* */recovery* – particija za oporavak omogućuje podizanje operativnog sistema mobilnog uređaja u konzoli za oporavak, a uz pomoć konzole se obavljaju aktivnosti poput ažuriranja telefona i drugih vrsta održavanja
* */system* – sve glavne komponente osim kernela i RAM-a su sačuvane na ovoj particiji
* */data* – ova particija se obično naziva particijom podataka i to je interno skladište podataka aplikacija gde se čuva većina korisničkih podataka
* */sdcard* – prostor koji je dostupan korisnicima za čuvanje svojih datoteka i podataka

Android operativni sistem može da koristi Linux 2.6 kernel ili SELinux kernel, koji obezbeđuje dodatnu bezbednosnu kontrolu. Fajl sistem se odnosi na način na koji se podaci čuvaju, organizuju i preuzimaju iz volumena. Svakom particijom može upravljati različiti fajl sistem i svaki fajl sistem definiše svoja pravila za upravljanje datotekama u volumenu. U zavisnosti od ovih pravila, fajl sistem nudi različitu brzinu za preuzimanje datoteka, bezbednost, veličinu itd. Popis svih fajl sistema na uređaju se može naći u datoteci */proc/filesystems* (*slika 3.2.*).



Slika 3.2. Struktura fajl sistema

U nastavku je dat pregled najvažnijih fajl sistema [2]:

* *rootfs* – najvažniji fajl sistem i predstavlja jednu od glavnih komponenti Androida, sadrži sve informacije potrebne za pokretanje uređaja
* *sysfs* – montira */sys* direktorijum koji sadrži informacije o konfiguraciji uređaja
* *devpts* – predstavlja interfejs za sesiju terminala na uređaju, montira se na */dev/pts*
* *cgroup* – omogućava pristup i definisanje različitih parametara jezgra
* *proc* – sadrži informacije o strukturama podataka jezgra, procesima i ostalim informacijama u */proc* direktorijumu
* *tmpfs* – privremeno skladišti podatke u RAM memoriju, što znači da kada se uređaj restartuje ili isključi ovi podaci više neće biti dostupni
* *EXT (eng*. *Extended File System)* – uveden je 1992. godine, bio je jedan od prvih fajl sistema i koristio je virtuelni fajl sistem. EXT2, EXT3 i EXT4 su naredne verzije ovog fajl sistema, a upravo je EXT4 najčešći tip fajl sistema novih Android uređaja
* *VFAT* – predstavlja proširenje FAT16 i FAT32 fajl sistema. Većina Android uređaja podržava FAT32 fajl sistem i ovo omogućava sistemima da lako čitaju, menjaju i brišu datoteke koje su na FAT32 fajl sistemu. Većina SD kartica je formatirana pomoću FAT32 fajl sistema
* *YAFFS2 (eng. Yet Another Flash File System 2)* – fajl sistem otvorenog koda koji je objavljen 2002. godine i namenjen za uređaje koji koriste NAND fleš memoriju. Koristi napredne metode „sakupljanja smeća“ (eng. garbage collection) kako bi brže počistio izbrisane podatke. Trenutno, YAFFS2 nije podržan u novijim verzijama kernela, ali određeni proizvođači ga i dalje podržavaju
* *F2FS (eng. Flash Friendly File System)* – Samsung ga je predstavio 2013. godine kao fajl sistem otvorenog koda. Osnovna namera je bila napraviti fajl koji uzima u obzir karakteristike uređaja za skladištenje na temelju NAND fleš memorije
* *RFS (eng. Robust file system)* - podržava NAND flash memoriju na Samsung uređajima. RFS je u sličan kao FAT16 ili FAT32 fajl sistem u kojem je zapisivanje omogućeno kroz transakcijski log. Mana je kašnjenje koje uzrokuje usporavanje celog Android operativnog sistema

# **Forenzika mobilnih uređaja**

Digitalna forenzika predstavlja primenu naučnih metoda u svrhu prikupljanja, identifikacije, analize, interpretacije i dokumentovanja dokaza iz digitalnih izvora koji podrazumevaju digitalne medijume za skladištenje podataka, kao i računarske sisteme.

Jedna od grana digitalne forenzike, forenzika mobilnih uređaja, postala je nezaobilazna u različitim postupcima i istragama, od privatnih, korporativnih pa do kriminalističkih. Potreba za pronalaženjem, oporavkom i analizom podataka u elektronskom obliku sve je veća, bilo da se radi o istraživanju zlonamernih postupaka ili istragama koje za cilj imaju povećanje korporativne sigurnosti podataka. Takođe je vrlo bitno napomenuti da se pod pojmom mobilnih uređaja ne nalaze samo mobilni telefoni, što je najčešća asocijacija. Pod pojmom mobilnih uređaja, u sklopu forenzike mobilnih uređaja, podrazumevaju se svi uređaji koji imaju sopstvenu unutrašnju memoriju i sposobnost komunikacije. Između ostalog to uključuje PDA (eng. Personal Digital Assistant) uređaje, GPS (eng. Global Positioning System) uređaje i tablete.

Osnovni princip digitalne forenzike (kao i forenzike mobilnih uređaja) je sačuvati originalni podatak od promena. Upravo ovaj princip je izuzetno teško ispuniti kod mobilnih uređaja jer su podaci „krhke“ prirode i lako mogu biti modifikovani, uništeni ili izgubljeni. Zbog takve prirode digitalnih podataka od velike je važnosti poštovati proceduru pribavljanja digitalnih dokaza te njihova obrada i pravilna prezentacija tokom nekog postupka.

Digitalnu forenziku mobilnih uređaja možemo podeliti na dva segmenta:

* forenziku memorije uređaja
* forenziku SIM kartice

Postoji velik broj različitih metodologija forenzike mobilnih uređaja, a jedna od najpoznatijih je NIST (eng. The National Institute of Standards and Technology) metodologija. Prema izvoru [1] iz 2014. godine NIST-ova metodologija se sastoji od sledećih faza: očuvanje (izolacija), prikupljanje (akvizicija), ispitivanje, analiza i izveštavanje.

**1. Faza očuvanja (izolacija)** je prva faza u procesu digitalnog prikupljanja podataka i podrazumeva oduzimanje i obezbeđivanje imovine osumnjičenog bez menjanja sadržaja podataka na uređajima. Nakon oduzimanja uređaja sa ciljem sprečavanja izmene sadržaja, ukoliko je telefon uključen, važno je izvršiti mrežnu izolaciju. Poželjno je telefon odložiti u Faradejevu kutiju/vrećicu, ali i onemogućiti sve mrežne veze (Wi-Fi, GPS, Hotspot, itd) i aktivirati režim letenja.

**2. Faza prikupljanja (akvizicija)** je druga faza u kojoj se sakupljaju informacije sa digitalnih uređaja. Podrazumeva identifikaciju i ekstrakciju podataka. Cilj ove faze je preuzimanje podataka sa mobilnog uređaja. Prvi korak je odrediti koji tip mobilne mreže uređaj koristi.

Danas su najrasprostranjenije sledeće mreže:

* CDMA (eng. Code Division Multiple Access) – ne poseduje SIM modul, svi podaci se nalaze i čuvaju na mobilnom uređaju, koristi se pretežno u SAD
* GSM (eng. Global System for Mobile Communication) – mreže koriste SIM module kao odvojene komponente dizajnirane da budu prenosive sa jednog telefona na drugi, koriste se u Evropi i nekim istočnim zemljama
* IDEN (eng. Integrated Digital Enhanced Network) – koristi sistem naprednih SIM kartica (USIM – Universal SIM)

Vrsta mobilne mreže koja se koristi u mobilnom uređaju direktno utiče na pristup koji se koristi prilikom dalje analize mobilnog telefona. Ukoliko se radi o GSM ili IDEN uređajima, sledeći korak je napraviti forenziku SIM kartice.

SIM omogućava korisniku prebacivanje podataka kao što su imenik, istorija poziva, poruka i sl. Najsigurniji način pristupa mobilnom telefonu je kloniranje SIM kartica korišćenjem forenzičkih alata. Obrisani podaci sa SIM kartice mogu se vratiti uz pomoć softverskih alata. Taj postupak nam je dostupan jer podatak obrisan iz memorije bilo to na SIM kartici ili uređaju nakon brisanja ne nestaje, već je označen kao slobodan prostor i čeka da se na njegovo mesto upiše novi podatak. Za to vreme njegov sadržaj je i dalje prisutan i može se pročitati.

Nakon utvrđivanja mreže u kojoj mobilni telefon radi, sledeći korak je utvrđivanje tipa mobilnog uređaja da bi se utvrdile njegove karakteristike i mogućnosti. Identifikacija tipa mobilnog telefona sprovodi se pretragom proizvođača, serijskog broja uređaja koji se obično nalaze ispod baterije, kodovima proizvođača. Kroz kod proizvođača moguće je doći do informacije kao što su: proizvođač telefona, model, kod države u kojoj je proizveden.

Forenzička ekstrakcija – izvlačenje podataka sa mobilnih uređaja je jedan od najzahtevnijih postupaka forenzičke istrage. Da bi se ona mogla pravilno izvesti, potrebno je znati kako je izvedena memorija na tom uređaju kako bi znali gde tražiti dokaze. Problem predstavlja mobilnost podataka jer oni zapravo mogu biti na drugoj lokaciji kao što je cloud okruženje, danas vrlo popularno kod mobilnih korisnika.

**3. Ispitivanje i analiza** **–** ova faza preuzima stečene podatke i vrši analizu nad njima kako bi se identifikovali delovi dokaza. Ona uključuje ispitivanje sadržaja datoteka i direktorijuma i oporavak izbrisanih sadržaja. Alati u ovoj fazi će analizirati fajl sistem za popis imena svih prikupljenih datoteka i prikazivanje podataka u najkorisnijem obliku za korisnike. Ispitivanje i analiza imaju za cilj da potvrde ili demantuju pretpostavke vezane za slučaj i da iz skupa dokaza povežu relevantne podatke za konkretan slučaj i formiraju sliku događaja.

**4. Faza izveštavanja** je završna faza prema NIST metodologiji. Izveštavanje se oslanja na detaljan pregled svih preduzetih koraka i donetih zaključaka tokom istrage. Ova faza obuhvata izradu pisanih izveštaja o rezultatima istraživanja, uključujući sve relevantne informacije i dokaze koji su prikupljeni tokom procesa. Takođe se prezentuju rezultati testiranja i ispitivanja i daju objašnjenja do kakvih se zaključaka došlo na osnovu prikupljenih dokaza.

Od svih navedenih faza prve dve se smatraju najvažnijim. Očuvanje i prikupljanje mogu da obezbede ključne dokaze i značajne smernice za nastavak istrage. Svaki korak mora biti sproveden sa izuzetnom pažnjom jer naredne faze ispitivanja u potpunosti zavise od toga koliko dobro su obavljene prve dve faze [1].

## **4.1. Izazovi mobilne forenzike**

Jedan od najvećih forenzičkih izazova kada je u pitanju mobilna platforma je činjenica da se podacima može pristupiti i da se mogu čuvati i sinhronizovati sa/na više uređaja. Kako su podaci ranjivi i mogu se brzo transformisati ili brisati na daljinu, potrebno je mnogo više napora za njihovo očuvanje. Neki od izazova su [9]:

* Hardverske razlike – tržište je preplavljeno različitim modelima mobilnih uređaja različitih proizvođača. Novi modeli se pojavljuju izuzetno često što zaista predstavlja izazov za forenzičare koji moraju biti u toku sa svim promenama. Osim toga, ugrađen prostor za skladištenje nije jednostavno ukloniti sa uređaja, za razliku od tradicionalnih desktop računara i servera
* Operativni sistem – za razliku od personalnih računara u kojima Windows već godinama dominira na tržištu, mobilni uređaji koriste različite operativne sisteme, uključujući Apple-ov iOS, Google Android, RIM BlackBerry OS, Microsoft Windows Mobile, HP webOS, Nokia Simbian OS i druge. Pored ovolikog broja operativnih sistema čak i u okviru njih postoje velike razlike između različitih verzija
* Ugrađena sigurnost – ugrađene bezbednosne funkcije pametnog telefona prisutne su na mnogim nivoima kako bi se zaštitili podaci i privatnost korisnika. Načini zaključavanja u današnjim pametnim telefonima mogu se razlikovati od jednostavnog četvorocifrenog PIN-a, pa do mnogo kompleksnijih i dugačkih kodova, šablona zaključavanja ili biometrije. Novije verzije operativnih sistema nude potpunu enkrpiciju diska, što može biti izuzetno problematično prilikom pokušaja prikupljanja podataka
* Mobilnost podataka (Cloud okruženje) – zbog generisanja velike količine podataka, uštede prostora za skladištenje ili potrebe za rezervnim kopijama, korisnici biraju da čuvaju puno važnih podataka u oblaku, pa se podaci zapravo ne nalaze na mobilnom uređaju
* Ranjivost podataka – generalna osobina digitalnih podataka je da mogu biti ranjivi, ali to posebno dolazi do izražaja kod mobilnih uređaja. Digitalni dokazi se mogu lako menjati (sa namerom ili ne), skroz modifikovati i umnožavati bez ostavljanja traga. Prilikom mrežnog prenosa, informacija može biti modifikovana ili izgubljena
* Generičko stanje uređaja – čak i ako se čini da je uređaj van stanja rada, pozadinski procesi mogu i dalje raditi. Na primer, kod većine mobilnih uređaja alarm i dalje radi čak i kad je uređaj isključen. Takođe, prelaz iz jedne države u drugu može dovesti do gubitka ili promene podataka
* Nedostatak dostupnosti alata – zbog širokog raspona mobilnih uređaja jedan alat možda ne podržava sve uređaje ili obavlja sve potrebne funkcije pa treba koristiti kombinaciju alata

## **4.2. Alati za forenziku mobilnih uređaja**

Osim odabira odgovarajućih metoda forenzičke istrage važno je odabrati odgovarajuće alate kojima će se sprovesti forenzička istraga. Vrlo često će biti potrebna kombinacija više alata kako bi se prikupili željeni podaci i ostvario željeni rezultat istrage.

Forenzički alati se mogu podeliti na:

* Hardverski alati – koriste se za direktan pristup podacima sa mobilnog uređaja i omogućavaju forenzičarima pristup podacima koji se inače ne mogu dobiti pomoću softverskih alata. Kreću se od jednostavnih jedno-namenskih komponenti do kompletnih forenzičkih računarskih sistema i servera
* Softverski alati – većina softverskih alata, tj. aplikacija je višenamenska i može obavljati različite zadatke u jednoj aplikaciji. Neki od njih mogu obraditi više uređaja istovremeno ili upravljati različitim operativnim sistemima

Kompanija Cellebrite smatra se jednom od najpopularnijih u području forenzike mobilnih uređaja. Razvija hardverske i softverske alate za sprovođenje forenzičke analize mobilnog uređaja. U nastavku su opisani nekoliko najpopularnijih alata kompanije Cellebrite [5].

*UFED Touch2 Ultimate (slika 4.1.)* je prenosna hardverska platforma za digitalnu forenziku koja omogućava rad iz laboratorije, sa udaljenog mesta ili sa terena. Može prikupljati slike, video zapise, logove poziva i bilo koji drugi oblik logičkih podataka sa mobilnih uređaja. Ima produženi vek trajanja baterije, a prikupljenim podacima se odmah može pristupiti.



Slika 4.1. UFED Touch2 Ulitimate

*UFED Cloud Analyzer* – softverski alat za analizu podataka sa društvenih mreža i aplikacija koje se koriste na mobilnim uređajima. *UFED Cloud Analyzer* omogućava istraživačima da pristupe podacima sa aplikacija kao što su Facebook, Google, iCloud, itd., takođe omogućava analizu i prezentaciju u obliku izveštaja.

*UFED Physical Analyzer* – softverski alat za analizu podataka sa fizičkih uređaja, uključujući podatke o pozivima, porukama, lokacijama, aplikacijama i drugim podacima.

*UFED InField Kiosk* – hardverski alat za brzo i sigurno preuzimanje podataka sa mobilnih uređaja u terenskim uslovima. *UFED InField Kiosk* omogućava istraživačima da preuzmu podatke sa uređaja u realnom vremenu, bez potrebe za fizičkim pristupom uređaju.

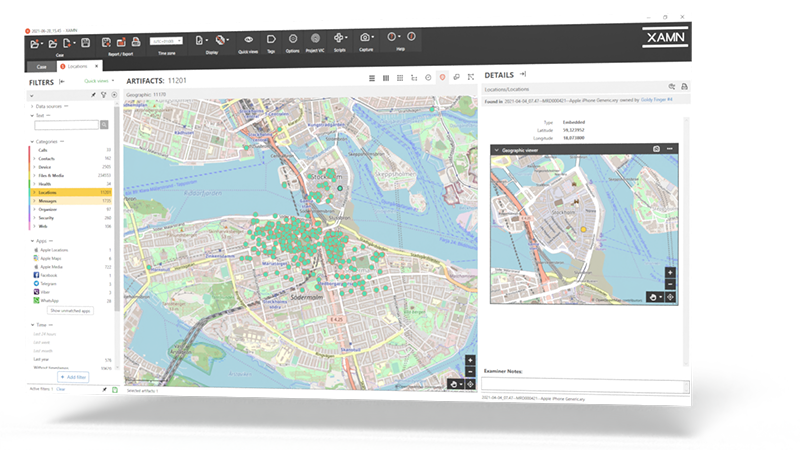
Osim navedenih Cellebrite softverskih alata, na tržištu su takođe popularni alati kompanija MSAB, EnCase, Autopsy, Oxygen Forensic.

MSAB nudi softverske alate na različitim hardverskim platformama, u nastavku su opisani nekoliko najpopularnijih alata za mobilnu forenziku koje je proizvela kompanija MSAB [6].

*XRY* se koristi za razne vrste ekstrakcije podataka sa mobilnih uređaja, kao što su logička ekstrakcija, fizička ekstrakcija, cloud ekstrakcija, itd.

*XRY PinPoint* omogućava ekstrakciju i dekodiranje podataka sa nestandardnih mobilnih uređaja, kao što su jeftine imitacije određenih proizvođača.

Osim proizvoda za ekstrakciju, MSAB također nudi proizvode poput *XRY kamere* koja omogućava snimanje digitalnih dokaza, kao i proizvode za analizu ekstrakovanih podataka (sa oznakom XAMN). To su proizvodi poput *XAMN Viewer*, *XAMN Spotlight*, *XAMN Elements*, *XAMN Horizon (slika 4.2.)*, itd.



Slika 4.2. XAMN Horizon

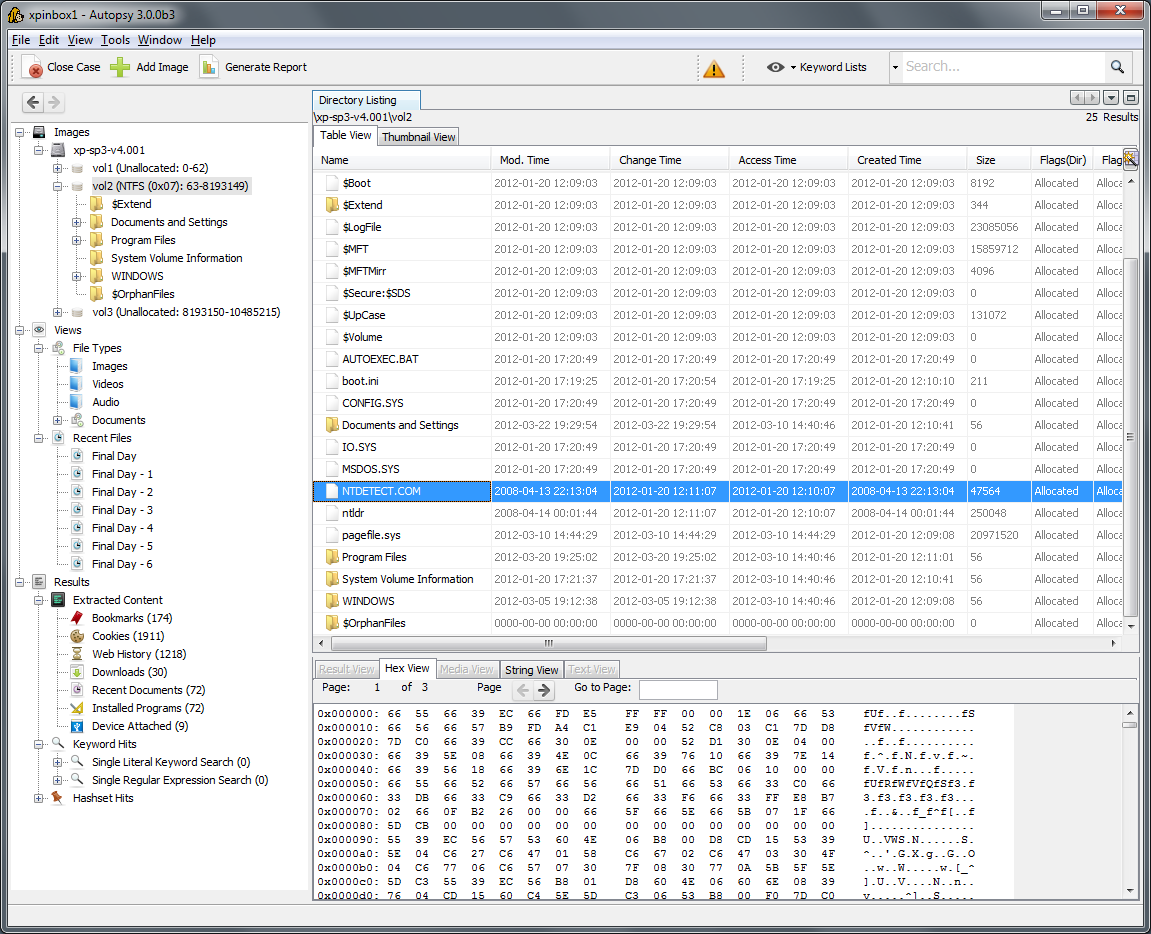
*EnCase Mobile Investigator* je proizvod kompanije EnCase koji omogućava bolji i lakši pregled različitih fajlova kao što su izbrisani fajlovi ili nealocirani prostori fajla.

*Autopsy* je alat istoimene kompanije koji se može koristiti za analizu podataka sa mobilnih uređaja koji imaju Android i iOS operativne sisteme. Alat sadrži određene module poput Android Analyzer Modula koji omogućava analizu SQLite baze podataka i drugih datoteka na Android uređajima. Navedeni modul ima mogućnost ekstrakcije tekstualnih poruka, kontakata, logova poziva, GPS podataka sa web pretraživača, Google Maps aplikacije i druge slične podatke. Takođe, alat sadrži dodatno i druge module vezane za ekstrakciju podataka sa mobilnih uređaja (*slika 4.3.*) [7].

Oxygen Forensic proizvodi više vrsta softverskih alata koji su namenjeni za ekstrakciju podataka sa mobilnih uređaja, dekodiranje i analizu ekstrakovanih podataka. U nastavku su opisani neki od najpopularnijih alata ove kompanije [8].

*Oxygen Forensic Detective* je softverski proizvod koji pruža kompletnu analizu podataka sa mobilnih uređaja.

*Oxygen Forensic Cloud Extractor* nudi brzu ekstrakciju podataka sa aplikacija poput WhatsApp, Telegram, Discord, Viber. Skeniranjem QR koda u aplikaciji na mobilnom telefonu, za nekoliko minuta možemo dobiti kompletan izveštaj sa ovih aplikacija na računaru. Takođe, postoji alat *Oxygen Forensic Viewer* koji omogućava forenzičarima deljenje ekstrakovanih podataka i analiziranih digitalnih dokaza.



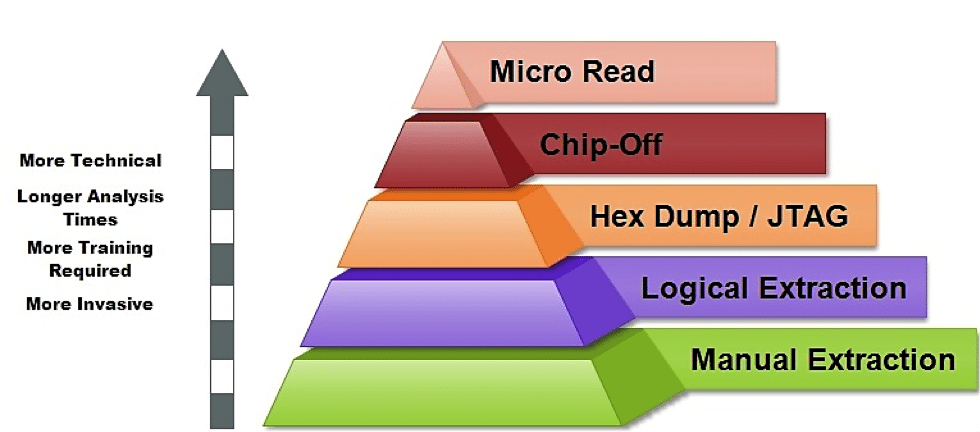
Slika 4.3. Autopsy alat

# **Metoda ekstrakcije**

Cilj forenzike memorije mobilnog uređaja je da se podaci koji su sačuvani u memoriji samog uređaja ekstrakuju i pronađu smisleni dokazi. Ekstrakcija podataka je postupak prikupljanja podataka, koji će kasnije moći da se koriste za dalju obradu i analizu. U digitalnoj forenzici mobilnih uređaja ovaj postupak je obavezan i u većini slučajeva je izuzetno značajan, jer omogućava dokaze ili druge važne podatke koji upućuju na dalje dokaze. O vrsti ekstrakcije koja će se primeniti u konkretnom slučaju odlučuje sam forenzičar. Odluku donosi pre svega na osnovu, tipa uređaja sa kojim radi, njegovog zatečenog stanja (ispravan, oštećen, zaključan i sl.), količine i vrste podataka koje želi izvući i forenzičkog alata/mogućnosti kojima raspolaže. Vrlo često, u praksi, važan faktor koji utiče na odluku je i vreme, jer je ponekad važnije što pre doći do određenih podataka. Najjednostavnijim metodama se može dobiti najmanje podataka, ali su najbrže, dok se najkomplikovanijim metodama može dobiti najviše podataka, ali je postupak dugotrajan, treba ispuniti posebne uslove u kojima se obavlja i zahteva skupu opremu, stručno osoblje i zbog toga je rezervisana za službe kao što su policija, vojska ili agencije koje se bave digitalnom forenzičkom analizom.

Postoji nekoliko vrsta ekstrakcije podataka mobilnih uređaja:

* Ručna ekstrakcija
* Logička ekstrakcija
* Fizička ekstrakcija
* Ostale metode ekstrakcije



Slika 5.1. Metode ekstrakcije podataka

Na *slici 5.1.* prikazane su metode ekstrakcije podataka sa mobilnih uređaja prema složenosti. U smeru strelice, odnosno prema vrhu piramide povećava se složenost sprovođenja ekstrakcije podataka, vreme analize, kao i stručnog znanja za sprovođenje iste.

## **5.1. Ručna ekstrakcija**

Ručna ekstrakcija je najjednostavnija metoda koja podrazumeva snimanje (obično digitalnom kamerom) svih informacija koje je moguće videti na ekranu mobilnog uređaja. Prednost ručne ekstrakcije je jednostavnost i brzina ekstrakcije, dok su glavni nedostaci količina ekstrakovanih podataka, mogućnost ljudske greške, moguće neuočavanje određenih ključnih digitalnih dokaza.

Jasno je da metoda efikasna samo u malom broju specifičnih slučajeva, jer ne nudi podatke kojima se ne može pristupiti kroz „sistem menija“, kao ni izbrisane podatke sa uređaja. Takođe, prilikom ručnog prikupljanja podataka uvek postoji rizik od slučajnog brisanja podataka koji su mogući digitalni dokazi. Osim navedenog, u slučaju oštećenja mobilnog uređaja, zaključanog uređaja ili sličnih situacija nije moguće sprovesti ručnu ekstrakciju. Ručnom ekstrakcijom moguće je prikupiti podatke poput kontakata, istorije poziva, SMS, MMS, e-mail poruke, istorije web pretraživača, video zapise, fotografije, dokumente, podatke sa društvenih mreža i sl., ukoliko su gore navedeni uslovi ispunjeni. Prikupljeni podaci mogu biti vidljivi odmah na računaru koji je povezan sa alatom. Na *slici 5.2.* prikazan je hardverski alat *Cellebrite UFED* kamera, koja omogućava ručno ekstrakovanje podataka. Pomoću *Cellebrite UFED* kamere sprovodi se ručna ekstrakcija podataka na način da se snima ekran mobilnog uređaja. Digitalni dokazi prikupljaju se snimanjem fotografija, video zapisa podataka, odnosno direktnim snimcima ekrana.



Slika 5.2. Cellebrite UFED kamera

## **5.2. Logička ekstrakcija**

Logička ekstrakcija je nakon ručne najlakša i najkompatibilnija metoda, ali povlači manji broj podataka od fizičke. Ovaj pristup podrazumeva povezivanje mobilnog uređaja i forenzičkog alata pomoću USB kabla, Bluetooth-a, WiFi-a, RJ-45 kabla i sl. Većina forenzičkih alata podržava logičku ekstrakciju, a sam proces je relativno jednostavan i zahteva kratkotrajnu obuku.

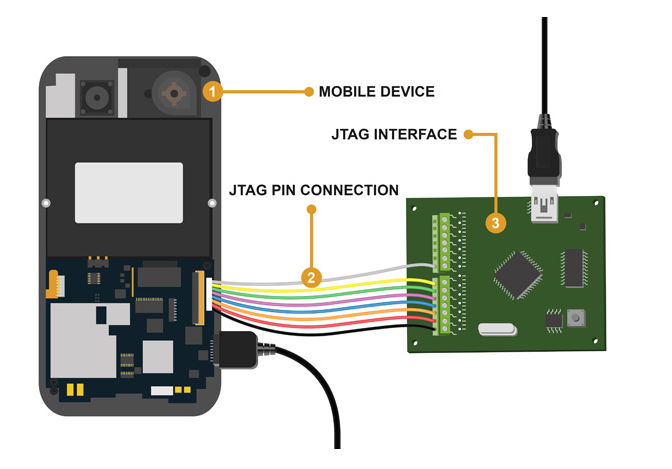
Nakon povezivanja uređaja sa računarom, računar inicira naredbu prema mobilnom uređaju. Naredba se interpretira od strane procesora mobilnog uređaja i nakon toga se traženi podaci šalju nazad prema računaru. Izbrisani podaci nisu dostupni logičkom ekstrakcijom. Takođe, logička ekstrakcija zahteva određeno poznavanje alata sa kojim se radi. Ovom metodom nije moguće zaobići zaključan ili zaštićen uređaj. Moguće je izvlačenje podataka logičkom ekstrakcijom i bez root pristupa, ali root pristup će omogućiti prikupljanje znatno većeg broja podataka. Kao prednosti logičke ekstrakcije podataka mogu se navesti jednostavnost i brzina ekstrakcije veće količine podataka u odnosu na ručnu ekstrakciju. Primer alata za ovakav oblik ekstrakcije su *MSAB XRY Logical* i *UFED Logical Analyzer* koji se primenjuju za ekstrakciju i analizu podataka. Logička ekstrakcija može se sprovesti sa prethodno navedenim alatima, a isto tako može se sprovesti pomoću adb naredbi. Korišćenjem adb naredbi mogu se izvući svi podaci sa uređaja ili samo podaci sa tražene lokacije. Za pristup uređaju preko adb potrebno je osigurati otključan uređaj i uključenu opciju „*USB Debugging*“. Podaci aplikacija mogu biti skladišteni na razne lokacije, kao što su: interna memorija, eksterna memorija, SQLite baza podataka, itd. Korišćenjem softvera *DB Browser for SQLite* olakšava se analiza ekstrakovanih podataka iz baze podataka, jer nudi tabelarni prikaz. Takođe, jedan od korisnih alata za analizu podataka prikupljenih iz baza podataka je alat *Oxygen Forensic Viewer*.

## **5.3. Fizička ekstrakcija**

Kompletan sadržaj memorije se iščitava uz pomoć nekog od uređaja bit-po-bit. Kao rezultat takvog kopiranja dobija se slika memorije u binarnom formatu. Zatim se utvrđuje lokacija gde se nalazi potreban podatak. Ovom metodomse dobija najviše podataka što uključuje podatke o lokaciji, podatke iz svih aplikacija, itd. Za razliku od logičkih procesa ekstrakcije, fizička metoda zaobilazi operativni sistem telefona prikupljajući podatke direktno iz unutrašnje flash memorije telefona. Prednost ove tehnike je što se kopira ne samo alocirani, nego i nealocirani prostor memorije, tj. uz postojeće podatke kopiraju se i oni izbrisani i odbačeni.

U fizičku ekstrakciju spadaju metode JTAG (eng. Join Test Action Group) i Chip-off. One ne zahtevaju ni administratorski pristup ni uključenu opciju „*USB Debugging*“, čime istovremeno rešavamo i problem zaključanog uređaja.

JTAG je napredna invazivna metoda fizičke ekstrakcije (*slika 5.3.*) koja koristi testne priključne portove (eng. test access ports – TAP) kako bi se ostvario pristup neobrađenim podacima sačuvanim na mobilnim uređajima. Ovaj proces uključuje korišćenje postojećih tački lemljenja na elektronskoj ploči. JTAG ekstrakcija podataka zahteva odgovarajuću opremu i odgovarajući JTAG kabl kako bi se mogla sprovesti ekstrakcija svih podataka sa mobilnog uređaja.



Slika 5.3. JTAG ekstrakcija

Sledeća invazivna fizička metoda ekstrakcije je Chip-off metoda. Chip-off metoda je učinkovita, ali destruktivna metoda zbog toga što zahteva uklanjanje, odnosno odlemljivanje čipa flash memorije uređaja i obično je poslednja opcija kada je u pitanju izvlačenje podataka sa uređaja. Ova metoda uključuje posebne procese i opremu kako bi se razdvojio memorijski čip i izvukli podaci za analizu. Prema količini ekstrakovanih podataka ova metoda približno je jednaka prethodno opisanoj JTAG metodi. Konačni rezultat je taj da je uređaj uništen, ali su podaci sačuvani.

## **5.4. Ostale metode ekstrakcije**

Micro Read postupak uključuje ručno gledanje i tumačenje podataka vidljivih na memorijskom čipu. Forenzičar koristi elektronski mikroskop i analizira fizičke ulaze na čip, a zatim prevodi status na 0 i 1 kako bi se odredili rezultujući ASCII znakovi. Ceo proces je dugotrajan i skup i zahteva veliko znanje i obuku na flash memoriji i fajl sistemu. Takođe, metoda je jako spora i zahteva složenu tehničku opremu. Metoda je dosta zastarela, ali prednost je da može izdvojiti sve podatke iz memorije uređaja i daje najbolju sliku o tome što se događa u uređaju.

Od ostalih metoda ekstrakcije možemo izdvojiti ekstrakciju Clouda koja je novija metoda, jer iako spada u izazove u velikoj meri pomaže u količini prikupljenih podataka i formiranju detaljnije slike. Problem predstavlja činjenica da je Cloud distribuirano okruženje i da računari od interesa nisu na istoj geografskoj lokaciji. Pored toga često je potrebno doći i do mrežnih zapisa kako bi se utvrdilo kada je podatak postavljen na Cloud. Olakšavajuća okolnost je to što se ne zahteva pristup samom uređaju i nije bitno da li je uređaj zaključan ili ne.

# **Android Debug Bridge (adb)**

Za forenzičke postupke na mobilnim uređajima sa Android operativnim sistemom najvažniju ulogu ima *adb* (engl. Android Debug Bridge). Android Debug Bridge je alat koji se koristi za povezivanje računara sa Android uređajem i za upravljanje uređajem iz komandne linije. Nalazi se na putanji: *<sdk\_lokacija>/platform-tools*. Da bi adb funkcionisao mora biti uključena opcija „*USB Debugging*“. Ona se nalazi u podešavanjima – *Developer Tools*, ali to ne mora biti tako na svim uređajima, budući da različiti uređaji imaju različita podešavanja. Pored toga na računaru je neophodno imati instaliran *adb* alat.

Jednom kada se uključi opcija „*USB Debugging*“, uređaj će pokrenuti adb daemon (adbd) u pozadini i neprestano će tražiti USB vezu. Daemon će se obično pokrenuti pod neprivilegovanim korisničkim nalogom i na taj način se ne omogućuje pristup internim podacima. Dok na mobilnim uređajima sa root pristupom adbd će se pokretati sa privilegijama root naloga i pružati pristup svim podacima. Na računaru (na kome je instaliran Android SDK) adbd će se pokrenuti kao pozadinski proces. Nakon povezivanja uređaja i pre pokretanja adb naredbi, korisno je znati da li je uređaj ispravno povezan na adb server. To se može proveriti pomoću naredbe *adb devices* koja pokazuje spisak svih uređaja koji su povezani na računaru (*slika 6.1.*).



Slika 6.1. Pretraga uređaja pomoću naredbe **adb devices**

Važno je imati na umu da ukoliko programi nisu instalirani, ili nisu ispravno instalirani, prethodna naredba će pokazati praznu liniju jer neće naći povezani uređaj. Kao što se vidi u rezultatima naredbe, odgovor te naredbe sadrži jedinstveni broj uređaja. Ovaj broj je jedinstveni niz koji koristi adb kako bi identifikovao svaki Android uređaj [10].

Moguće vrednosti stanja veze i njihovo značenje su sledeće:

* offline – instanca nije povezana na adb ili ne reaguje
* device – instanca je povezana na adb server
* no device – nije povezan uređaj

Ako je povezano više uređaja moramo navesti jedinstveni broj uređaja kome prosleđujemo naredbe. To možemo učiniti tako što posle ključne reči *adb* dodamo opciju *-s* i navedemo broj uređaja (*slika 6.2.*), koji je rezultat prethodne naredbe sa *slike 6.1.*



Slika 6.2. Primer izvšavanja **adb install** naredbe na određenom uređaju

Ukoliko želimo da proverimo da li na priključenom uređaju postoji root pristup. To se izvodi pokretanjem naredbe *adb shell*. Ovom naredbom će se otvoriti shell prema mobilnom uređaju i on će komunicirati sa računarom, što znači da bilo koja naredba koje se izvrši u shell-u, izvršiće se i na mobilnom uređaju. Shell će se pojaviti na jedan od dva načina, bilo sa **$** ili **#**. U Linux sistemima **#** se koristi za označavanje root korisnika, a **$** označava korisnika koji nije root. Ako shell vraća znak **#**, ima root pristup. Ako shell vrati **$**, pokušajte pokrenuti naredbu *su*. Ako je *su* naredba podržana na uređaju, shell će preći u root pristup. Lokacije „bitnijih“ podataka koji su skladišteni na uređaju možemo pronaći u *tabeli 1.*

Tabela 1. Pregled tipova podataka i lokacija na kojima su skladišteni

|  |  |
| --- | --- |
| Tip podatka | Lokacija |
| Podaci o uređaju | /system/build.prop |
| Kontakti | /data/data/com.android.providers.contacts/databases/contacts2.db |
| Istorija poziva | / data/data/com.android.providers.contacts/databases/calllog.db |
| SMS/MMS | /data/data/com.android.providers.telephony/databses/mmssms.db |
| E-pošta | /data/data/com.android.email/databases/emailprovider.db |
| Istorija pretraživača | /data/data/com.android.browser/databases/browser2.db |
| Kalendar | /data/data/com.android.providers.calendar/databases/calendars.db |

Kada imamo pripremljeno okruženje naredba *adb pull* može se koristiti za kopiranje fajlova/foldera na računar forenzičara, dok naredba *adb push* služi za kopiranje fajlova/foldera sa računara na mobilni uređaj (*slika 6.3.*).



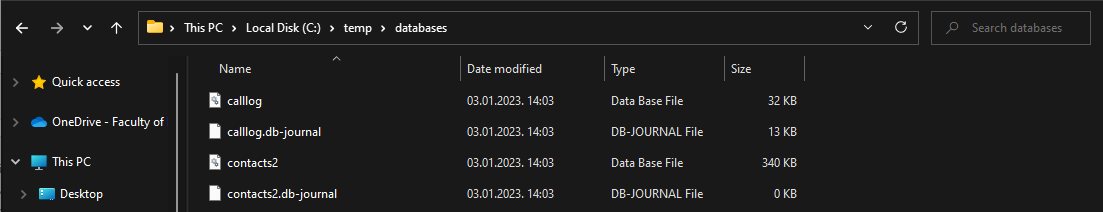
Slika 6.3. Sintaksa naredbi **adb pull** i **adb push**

Na primeru ćemo pokazati ekstrakciju kontakata i istorije poziva koji se nalaze u fajlovima *contacts2.db* i *calllog.db.* Najpre ćemo iskoristiti naredbu *adb pull* da izvučemo sve podatke iz foldera */data/data/com.android.providers.contacts/databases* u folder *C:\temp* na lokalnom računaru (*slika 6.4.*).



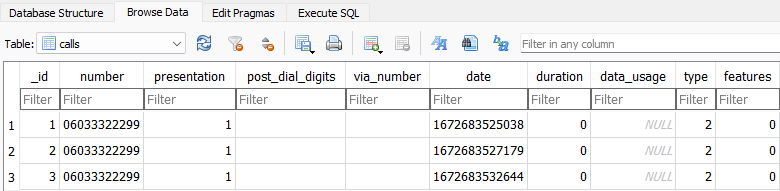
Slika 6.4. Primer korišćenja naredbe **adb pull**

Nakon izvršenja ove naredbe povratna vrednost će biti broj uspešno ili neuspešno iskopiranih fajlova, pa možemo otići da odredišnu lokaciju i videti da su traženi fajlovi uspešno iskopirani na računaru (*slika 6.5.*).

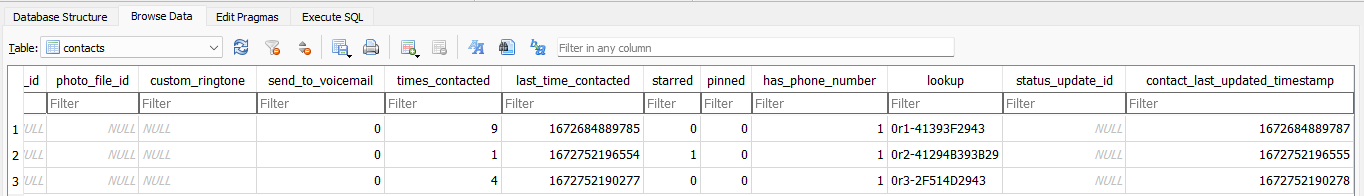


Slika 6.5. Pregled ekstrakovanih podataka na računaru

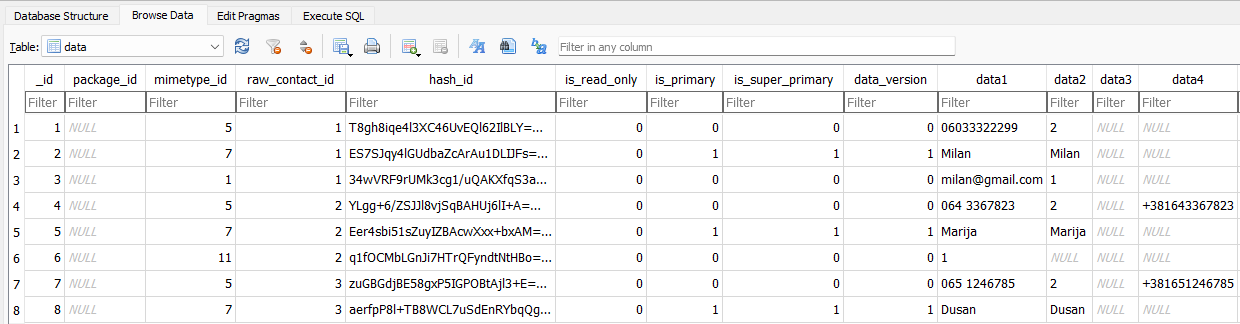
Nakon toga možemo izvršiti pregled i analizu dobijenih podataka. Ekstenzija ovih fajlova je *.db*, pa ćemo iskoristiti alat *DB Browser for SQLite* koji može otvoriti ove fajlove. Istorija poziva se nalazi u tabeli *calls*, gde su prikazani važni podaci o pozivima (broj, datum i vreme, trajanje, tip – dolazni, odlazni, propušteni, itd.) – *slika 6.6.*, dok se lista kontakata nalazi u tabeli *contacts* (*slika 6.7.*), a detaljne informacije o njima u tabeli *data* (*slika 6.8.*).



Slika 6.6. Pregled tabele **calls**



Slika 6.7. Pregled tabele **contacts**



Slika 6.8. Pregled tabele **data**

Na ovaj način možemo izvršiti ekstrakciju i ostalih tipova podataka navedenih u *tabeli 1.*, kao i drugih tipova, samo je potrebno znati lokaciju gde se nalaze. Od ostalih adb naredbi možemo izdvojiti *adb install* koja instalira prosleđeni APK na uređaju (*slika 6.2.*), *screencap* koja pravi snimak ekrana uređaja, *screenrecord* koja pokreće snimanje ekrana uređaja [10].

# **Zaključak**

Mobilni uređaji u današnje vreme predstavljaju vrlo značajan izvor informacija. Čitava komunikacija odvija se putem mobilnih uređaja, čime oni postaju baza podataka korisnika. Pomoću forenzičke analize mobilnog uređaja može se doći do raznih podataka kao što su istorija poziva i poruka, fotografije, istorija pretraživača, izbrisani podaci i ostali podaci koji se mogu koristiti kao oblik digitalnog dokaza u mogućim sudskim procesima. Postoje razni tipovi ekstrakcije podataka koji mogu prikupiti veći ili manji broj potrebnih podataka u zavisnosti od složenosti i vremenu potrebnom za izvršavanje. Ručna ekstrakcija podataka zahteva najmanje vremena i stručnog znanja, dok fizička ekstrakcija zahteva stručno znanje i više vremena za njeno izvršavanje, ali i daje najviše podataka kao rezultat celog procesa.

Uprkos činjenici da postoji mnoštvo podataka i dosta različitih metoda ekstrakcije brojni izazovi mogu uticati na količinu prikupljenih podataka i brzinu rada. Hardverske i softverske razlike kod različitih proizvođača su očekivane, ali se pojavljuju i kod istih modela uređaja na unapređenim verzijama. Ranjivost podataka je potencijalno ugrožena bežičnim pristupom na Cloud rešenja. Sami proizvođači mobilnih uređaja konstantno unapređuju zaštitu podataka na svojim uređajima pa dodatno otežavaju ekstrakciju podataka.

Pored odabira odgovarajućih metoda važno je odabrati i odgovarajuće alate, a često je potrebna kombinacija više alata kako bi se prikupili željeni podaci. Forenzički alati se mogu podeliti na hardverske koji su skuplji, brži, pouzdaniji i softverske koji su fleksibilniji i jeftiniji. Možemo izdvojiti nekoliko proizvođača koji prednjače u ovoj industriji. Kompanija Cellbrite sa alatima *UFED Cloud Analyzer* i *UFED Touch2 Ultimate*, kompanija MSAB sa alatima *XRY* i *XAMN*, kompanija EnCase sa alatom *EnCase Mobile Investigator*, kao i kompanije Autopsy i Oxygen Forensic sa istoimenim alatima.

Za sprovođenje logičke ekstrakcije možemo iskoristiti besplatan *adb* alat, tj. pomoću adb naredbi možemo izvršiti izvlačenje pojedinih datoteka ili čitavih direktorijuma na računar. Problem može biti zaključan uređaj, jer je potrebno uključiti opciju „*USB Debugging*“. Za pristup svim podacima potrebno je imati i root pristup, a da bismo znali sa kojih lokacija treba izvući podatke potrebno je biti upoznat sa arhitekturom Android operativnog sistema, kao i sa strukturom fajl sistema.

# **Literatura**

1. Ayers R., Brothers S., Jansen W. (2014): *Guidelines on Mobile Device Forensics*, SAD, NIST Special Publication 800-101
2. Tamma R., Skulkin O., Mahalik H., Bommisetty S. (2018): *Practical Mobile Forensics Third Edition*, Birmingham - UK, Packt Publishing
3. Number of smartphone subscriptions worldwide from 2016 to 2021, with forecasts from 2022 to 2027, <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/> (pristupljeno: 10.12.2022.)
4. Android Platform Architecture, <https://developer.android.com/guide/platform> (pristupljeno: 23.12.2022.)
5. Cellebrite Platforms, <https://www.cellebrite.com/en/platforms/> (pristupljeno: 24.12.2022.)
6. MSAB Products, <https://www.msab.com/products/> (pristupljeno: 24.12.2022.)
7. Autopsy, <https://www.autopsy.com/> (pristupljeno: 25.12.2022.)
8. Oxygen Forensic, <https://www.oxygen-forensic.com/en/> (pristupljeno: 25.12.2022.)
9. Lillis D., Becker B., O'Sullivan T., Scanlon M. (2016): *Current Challenges and Future Research Areas for Digital Forensic Investigation*, University College Dublin, Ireland
10. Android Debug Bridge (adb), <https://developer.android.com/studio/command-line/adb> (pristupljeno: 2.1.2023.)