

Univerzitet u Nišu

Elektronski Fakultet

Forenzička analiza Android aplikacija korišćenjem AndroidDebugBridge-a

Predmet: Digitalna fornzika

Student: Profesor:

Aleksandar Mitrović 1444 Prof. dr Bratislav Predić

**Sadržaj**

1 Upoznavanje sa Android forenzikom………………………….…………….3

1.1 Mobilna forenzika……………………………………................……4

1.2 Izazovi u mobilnoj forenzici…………………………….……………6

2 Postavljanje radnog okruženja………………………………........…………8

2.1 Andoid Debug Bridge……………………………….....…………….9

2.2 Root-ovanje……………………………………....................………10

2.3 Recovery I Fastboot mod……………………......…………………12

3 Razumevanje prostora podatka na Androidu………...……………………14

3.1 Raspored particija……………………………..................…………14

3.2 Hijerarhija fajlova…………………………...................……………15

4 Logička ekstrakcija podataka…………………………….............…………21

4.1 Šta moze da se spasi? …………………………....................……22

4.2 ADB dumpsys…………………………………........................……23

4.3 Zaobilaženje Android ekrana za zaključavanje...........................26

5 Fizićka ekstrakcija podataka……………………..............…………………27

5.1 Generalni pregled………………………..................………………27

5.2 Rad sa komandom dd……………………...........…………………28

6 Forenzička analiza aplikacija na uredjaju………............…………………29

7 Pregled gotovih alata iz ove oblasti………………...………………………31

7.1 ViaExtract………………………………..........................…....……31

7.2 Autopsy………………………………….................................……32

7.3 ViaLab……………………………….................................…..……34

8 Literatura.................................................................................................37

**Upoznavanje sa Android forenzikom**

Forenzika mobilnih uređaja je grana digitalne forenzike koja se bavi izdvajanjem, vraćanjem i analizom digitalnih dokaza ili podataka sa mobilnog uređaja u forenzički zdravim uslovima. Bavi se pristupom podacima uskladištenim na uređajima koji uključuju SMS, kontakte, evidenciju poziva, fotografije, video zapise, dokumente, datoteke aplikacija, istoriju pregledanja i tako dalje, kao i vraćanje podataka izbrisanih sa uređaja pomoću različitih forenzičkih tehnika. Važno je da proces vraćanja ili pristupa detaljima sa uređaja bude forenzički ispravan, ako mora da bude prihvaćen pred sudom i da bi se održao integritet dokaza. Ako se dokazi moraju prihvatiti na sudu, važno je da se originalni uređaj ne menja.

Forenzička ispravnost nije samo u tome da originalni dokazi ostanu nepromenjeni. Čak i rutinski zadatak sticanja podataka sa diska pomoću hardverskog blokatora pisanja može izazvati izmene (na primer, omogućavanje pristupa skrivenom delu) na disku. Jedan od ključeva forenzičke ispravnosti je dokumentacija.

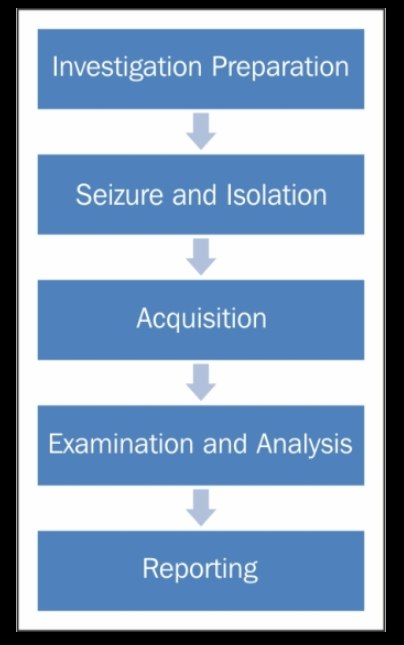
Dokumentovanje načina na koji se uređaj rukuje od početka je veoma važno. Dakle, istraga se može smatrati forenzički ispravnom ako proces akvizicije čuva originalne podatke i ako se njihova autentičnost i integritet mogu potvrditi. Provere integriteta dokaza obezbeđuju da dokazi nisu menjani od trenutka kada su prikupljeni. Provere integriteta se vrše upoređivanjem digitalnog otiska dokaza uzetih u vreme prikupljanja sa digitalnim otiskom dokaza u trenutnom stanju.

Postoji sve veća potreba za mobilnom forenzikom iz nekoliko razloga. Neki od istaknutih razloga su:

• Korišćenje mobilnih telefona za čuvanje ličnih podataka

• Povećana upotreba mobilnih telefona za obavljanje onlajn aktivnosti

• Upotreba mobilnih telefona u više krivičnih dela

**Mobilna forenzika**

Faze u mobilnoj forenzici

**Priprema za istragu**

Ova faza počinje kada se primi zahtev za ispitivanje. To uključuje pripremu sve papirologije i obrazaca potrebnih za dokumentovanje lanca čuvanja, informacija o vlasništvu, modela uređaja, njegove svrhe, informacija koje tražilac traži, itd. Lanac čuvanja odnosi se na hronološku dokumentaciju ili papirni trag, koji pokazuje zaplenu, čuvanje, kontrolu, prenos, analizu i raspolaganje fizičkim ili elektronskim dokazima. Na osnovu detalja koje dostavlja podnosilac zahteva, važno je imati jasno razumevanje cilja svakog ispitivanja.

**Zaplena i izolacija**

Rukovanje uređajem tokom zaplene jedan je od važnih koraka prilikom obavljanja forenzičke analize. Dokazi se obično transportuju korišćenjem antistatičkih vreća koje su dizajnirane da zaštite elektronske komponente od oštećenja izazvanih statičkim elektricitetom. Čim se uređaj zapleni, treba voditi računa da naše radnje ne dovedu do bilo kakve izmene podataka na uređaju. Istovremeno, ne treba propustiti svaku priliku koja može pomoći istrazi.

U mobilnoj forenzici, od kritične je važnosti da se zaštiti zaplenjeni uređaj tako da naša interakcija sa dokazima (ili u tom slučaju pokušaj napadača da daljinski stupi u interakciju sa uređajem) ne promeni dokaze. U kompjuterskoj forenzici imamo softverske i hardverske blokatore pisanja koji mogu da obavljaju ovu funkciju. Ali u mobilnoj forenzici, pošto moramo da komuniciramo sa uređajem da bismo izvukli podatke, ovi blokatori pisanja nisu od nikakve koristi. Još jedan važan aspekt je da takođe treba da sprečimo da uređaj komunicira sa bežičnim radio mrežama. Kao što je ranije pomenuto, postoji velika verovatnoća da napadač može izdati komande za daljinsko brisanje za brisanje svih podataka, uključujući e-poštu, aplikacije, fotografije, kontakte i druge datoteke na uređaju.

**Nabavka**

Faza nabavke se odnosi na ekstrakciju podataka sa uređaja. Zbog inherentnih bezbednosnih karakteristika mobilnih uređaja, izdvajanje podataka nije uvek jednostavno. U zavisnosti od operativnog sistema, marke i modela uređaja, odlučuje se o načinu ekstrakcije. Sledeći tipovi metoda akvizicije mogu se koristiti za izdvajanje podataka sa uređaja:

**Ručna akvizicija**: Ovo je najjednostavniji od svih metoda akvizicije. Ispitivač koristi korisnički interfejs telefona da pregleda i istražuje. Ovde nisu potrebni nikakvi specijalni alati ili tehnike, ali ograničenje je da se mogu izdvojiti samo one datoteke i podaci koji su vidljivi kroz normalan korisnički interfejs. Podaci izvučeni drugim metodama takođe se mogu verifikovati pomoću ovoga.

**Logička akvizicija**: Ovo se takođe naziva logičko izvlačenje. Ovo se generalno odnosi na ekstrakciju datoteka koje su prisutne u logičkom skladištu kao što je particija sistema datoteka. Ovo uključuje dobijanje tipova podataka, kao što su tekstualne poruke, istorija poziva, slike i tako dalje, sa telefona. Tehnika logičke ekstrakcije funkcioniše korišćenjem API-ja originalnog proizvođača opreme za sinhronizaciju sadržaja telefona sa računarom.

**Fizička akvizicija**: Ovo uključuje pravljenje bit-po-bit kopije cele fleš memorije. Podaci ekstrahovani ovim metodom obično su u obliku sirovih podataka (kao heksadecimalni dump), koji se zatim mogu dalje raščlaniti da bi se dobile informacije o sistemu datoteka ili podaci čitljivi ljudi. Pošto se sva istraživanja vrše na ovoj slici, ovaj proces takođe osigurava da se originalni dokazi ne menjaju.

**Ispitivanje i analiza**

U ovoj fazi se koriste različiti softverski alati za izdvajanje podataka iz memorijske slike. Pored ovih alata, istraživaču bi takođe bila potrebna pomoć heksadecimalnog uređivača, jer alati ne izvlače uvek sve podatke. Ne postoji jedinstven alat koji se može koristiti u svim slučajevima. Dakle, ispitivanje i analiza zahteva dobro poznavanje različitih sistema datoteka, zaglavlja datoteka itd.

**Izveštavanje**

Dokumentacija o ispitivanju treba da se vodi tokom celog procesa, beležeći šta je urađeno u svakoj fazi. Ispitivač može dokumentovati sledeće tačke:

* Datum i vreme početka ispitivanja
* Fizičko stanje telefona
* Status telefona kada je primljen (ON/OFF)
* Marka, model i operativni sistem telefona
* Slike telefona i pojedinih komponenti
* Alati koji se koriste tokom istrage
* Podaci dokumentovani tokom pregleda

**Izazovi u mobilnoj forenzici**

Sa povećanom upotrebom Android uređaja i širim spektrom komunikacionih platformi koje oni podržavaju, potražnja za forenzičkim pregledima je automatski porasla. Dok rade sa mobilnim uređajima, forenzički analitičari se suočavaju sa brojnim izazovima. Sledeće tačke bacaju svetlo na neke od izazova mobilne forenzike sa kojima se danas suočavaju:

**Sprečavanje izmene podataka na uređaju**: Jedno od osnovnih pravila koje treba zapamtiti u forenzici je da se dokazi ne menjaju. Drugim rečima, forenzičke tehnike koje se primenjuju na uređaj za izdvajanje bilo kakve informacije ne bi trebalo da menjaju podatke prisutne na uređaju. Ali ovo nije praktično u pogledu mobilne forenzike jer jednostavno uključivanje uređaja može takođe promeniti određene promenljive stanja koje su prisutne na uređaju. Kod mobilnih uređaja, pozadinski procesi se uvek pokreću i iznenadni prelazak iz jednog stanja u drugo može dovesti do gubitka ili modifikacije podataka. Stoga postoji šansa da forenzički analitičar namerno ili nenamerno promeni podatke.

Pored toga, postoji velika mogućnost da napadač može daljinski da promeni ili izbriše sadržaj koji se nalazi na uređaju. Kako mobilni telefoni koriste različite komunikacione kanale (ćelijski, Vi-Fi, Bluetooth, infracrveni i tako dalje), mogućnost komunikacije preko njih treba eliminisati. Funkcije kao što je daljinsko brisanje podataka omogućile bi napadaču da daljinski obriše ceo uređaj samo slanjem SMS-a ili jednostavnim pritiskom na dugme koje šalje zahtev za brisanje Android uređaju. Za razliku od kompjuterske forenzike, forenzika mobilnih uređaja zahteva više od pukog izolovanja uređaja od mreže.

**Širok spektar operativnih sistema i modela uređaja**: Širok spektar mobilnih operativnih sistema dostupnih na tržištu otežava život forenzičkog analitičara. Iako je Android najdominantniji operativni sistem u mobilnom svetu, postoje mobilni uređaji koji rade na drugim operativnim sistemima, uključujući iOS, Blackberri, Vindovs i tako dalje, koji se često susreću tokom istraga. Takođe za dati operativni sistem, dostupni su milioni mobilnih uređaja koji se razlikuju po verzijama OS-a, hardveru i raznim drugim funkcijama.

Na primer, u okviru Android operativnog sistema postoji oko 10 verzija, a za svaku verziju postoje različita prilagođavanja različitih proizvođača. U zavisnosti od proizvođača, pristup sticanju forenzičkih artefakata se menja. Da bi ostali konkurentni, proizvođači objavljuju nove modele i ažuriranja tako brzo da je teško pratiti sve njih. Ponekad se u okviru istog operativnog sistema menjaju i opcije skladištenja podataka i strukture datoteka, što ga čini još težim. Ne postoji jedinstven alat koji može da radi na svim dostupnim tipovima mobilnih operativnih sistema. Zbog toga je ključno da forenzički analitičari budu u toku sa svim najnovijim promenama i tehnikama.

**Nasledjene sigurnosne karakteristike:** Kako koncept „privatnosti“ sve više dobija na značaju, proizvođači mobilnih uređaja se kreću ka implementaciji robusnih sigurnosnih kontrola na uređajima, što komplikuje proces dobijanja pristupa podacima. Na primer, ako je uređaj zaštićen lozinkom, forenzički istražitelj mora prvo da pronađe način da zaobiđe lozinku. Slično tome, mehanizmi za šifrovanje punog diska koji su implementirani na nekim od najnovijih uređaja sprečavaju agencije za sprovođenje zakona i forenzičke analitičare da pristupe informacijama na uređaju. Apple-ov iPhone podrazumevano šifruje sve podatke prisutne na uređaju, koristeći hardverske ključeve ugrađene u uređaj. Ispitivaču je veoma teško da razbije ove mehanizme šifrovanja koristeći tehnike kao što je gruba sila.

**Pravna pitanja**: Mobilni uređaji mogu biti uključeni u zločine koji se protežu širom sveta i mogu da pređu geografske granice. Da bi se pozabavio ovim multijurisdikcijskim pitanjima, forenzičar mora biti svjestan prirode zločina, kao i regionalnih zakona.

**Postavljanje radnog okruženja**

Važno je da počnemo diskusiju sa Android SDK-om. Komplet za razvoj softvera za Android (SDK) pomaže programerima da naprave, testiraju i otklanjaju greške u aplikacijama koje će raditi na Androidu. Uključuje softverske biblioteke, API-je, emulator, referentni materijal i mnoge druge alate. Ovi alati ne samo da pomažu u kreiranju Android aplikacija, već takođe pružaju dokumentaciju i uslužne programe koji značajno pomažu u forenzičkoj analizi Android uređaja. Dobro poznavanje Android SDK-a može vam pomoći da razumete detalje uređaja. Ovo će vam, zauzvrat, pomoći tokom istrage.

Tokom forenzičkog pregleda, SDK nam pomaže da povežemo uređaj i pristupimo podacima prisutnim na uređaju.

Pre nego što započnete instalaciju Android SDK-a, uverite se da sistem ima instaliran Java Development Kit (JDK), jer Android SDK zavisi od Java SE Development Kit-a.

Sa instaliranim Android SDK-om, možete kreirati **Android virtuelni uređaj** (AVD), koji je emulator koji radi na radnoj stanici. Programeri često koriste emulator prilikom kreiranja novih aplikacija. Međutim, emulator se takođe smatra korisnim tokom forenzičkih istraga. Omogućava istraživaču da razume kako se određene aplikacije ponašaju i kako instalacija aplikacije utiče na uređaj. Još jedna prednost je što možete dizajnirati emulator sa željenom verzijom. Ovo je posebno korisno kada radite sa uređajima koji rade na starijim verzijama Android-a. Takođe, AVD podrazumevano dolazi sa root-om.

Da biste izvukli informacije sa Android uređaja, on prvo treba da bude povezan sa radnom stanicom. Kao što je ranije pomenuto, treba voditi računa da se uveri da je radna stanica forenzički sterilna i da se koristi samo u svrhu istrage. Forenzički sterilna radna stanica je ona koja ima ispravnu konstrukciju i ne sadrži viruse i drugi zlonamerni softver.

Android uređaj se može povezati sa radnom stanicom pomoću fizičkog USB interfejsa uređaja. Ovaj fizički USB interfejs omogućava uređaju da se povezuje, deli podatke i puni sa računara.

starijim Android uređajima je potreban USB režim masovne memorije za prenos datoteka između računara i uređaja. Najnoviji Android uređaji koriste Media Transfer Protocol (MTP) ili Picture Transfer Protocol (PTP), jer je bilo nekih problema sa USB protokolom za masovno skladištenje.

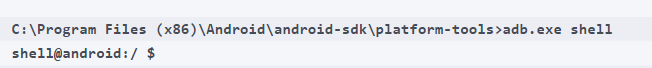
**Android Debug Bridge**

U Android forenzici, **Android Debug Bridge (ADB)** igra veoma ključnu ulogu. Prisutan je na *<sdk\_path>/platform-tools*. Da biste radili sa ADB-om, potrebno je omogućiti opciju **USB-debugging**. Na Samsung telefonu, ovome možete pristupiti tako što ćete otići u Podešavanja | Opcije programera;

Kada se izabere opcija za USB otklanjanje grešaka, uređaj će pokrenuti adb demon (adbd) u pozadini i stalno će tražiti USB vezu. Demon obično radi pod neprivilegovanim korisničkim nalogom ljuske i stoga ne pruža pristup internim podacima aplikacije. Međutim, na telefonima sa root-om, adbd će raditi pod root nalogom i na taj način će obezbediti pristup celokupnim podacima.

Deamon-i komuniciraju preko svog lokalnog domaćina na portovima 5555 do 5585

Koristeći ADB, možete pristupiti ljusci za pokretanje nekoliko komandi na Android uređaju.

Komanda *adb shell* se može koristiti za ulazak u udaljen shell, kao što je prikazano u sledećem izlazu komandne linije. Kada uđete u shell, možete izvršiti većinu Linux komande

Tokom forenzičke analize, može doći do slučajeva da morate da instalirate nekoliko aplikacija na uređaj da biste izdvojili neke podatke. Da biste to uradili, možete koristiti komandu za instalaciju *adb.exe install*. Zajedno sa ovom komandom, kao što je prikazano u sledećem izlazu komandne linije, potrebno je da navedete putanju do .apk datoteke koju želite da instalirate

Možete da koristite komandu *adb pull* da povučete datoteke prisutne na Android uređaju na lokalnu radnu stanicu.

**Rootovanje**

Da biste razumeli rutovanje, neophodno je razumeti kako funkcionišu sistemi slični Unix-u. Originalni Unik operativni sistem na kome su zasnovani Linux i drugi sistemi slični Unix-u dizajniran je od samog početka kao višekorisnički sistem. To je prvenstveno zbog toga što personalni računari još nisu postojali, pa je stoga bilo neophodno imati mehanizam za razdvajanje i zaštitu resursa pojedinačnih korisnika, a da im se omogući da sistem istovremeno koriste. Međutim, za obavljanje privilegovanih zadataka, kao što su davanje i ukidanje ovlašćenja za obične korisnike, pristup kritičnim sistemskim fajlovima za popravku ili nadogradnju sistema i tako dalje, bilo je neophodno imati nalog administratora sistema koji ima pristup superkorisnika. Dakle, imamo dve vrste naloga: normalne korisničke naloge, koji imaju manje privilegija, i superkorisnički ili root nalog, koji imaju sve privilegije.

Dakle, root je korisničko ime ili nalog koji podrazumevano ima pristup svim komandama i datotekama na Linux-u ili drugom operativnom sistemu sličnom Unix-u. Takođe se naziva i osnovni nalog, root korisnik i superkorisnik. Dakle, u Linux, root korisnik ima moć da pokrene ili zaustavi bilo koju sistemsku uslugu, izmeni ili izbriše bilo koju datoteku, promeni privilegije drugih korisnika itd. Android koristi jezgro Linux-a, pa je stoga većina koncepata prisutnih u Linux-u primenljiva i na Android. Međutim, kada kupite Android telefon, obično vam ne dozvoljava da se prijavite kao root korisnik. Rutovanje Android telefona se odnosi na dobijanje ovog root pristupa na uređaju za obavljanje radnji koje inače nisu dozvoljene na uređaju.

Takođe je važno razumeti razliku između root-a i jailbreakinga, jer se često pogrešno pretpostavlja da su isti. Jailbreaking uređaja koji pokreće Apple iOS omogućava vam da uklonite određena ograničenja i ograničenja koja je postavio Apple. Na primer, Apple nam ne dozvoljava da učitamo nepotpisanu aplikaciju na uređaj. Dakle, jailbreakingom možete instalirati aplikacije koje Apple nije odobrio. Nasuprot tome, Android dozvoljava bočno učitavanje aplikacija. Jailbreaking telefona uključuje zaobilaženje nekoliko sigurnosnih ograničenja istovremeno. Stoga je dobijanje root pristupa na uređaju samo jedan od aspekata Jailbreaking-a

**Šta je root**

Rutovanje često obavljaju mnogi ljudi sa ciljem prevazilaženja ograničenja koja operateri i proizvođači hardvera postavljaju na Android uređaje. Rutovanjem Android uređaja možete da promenite ili zamenite sistemske aplikacije i podešavanja, da pokrenete specijalizovane aplikacije koje zahtevaju dozvole na nivou administratora ili da obavljate operacije koje inače nisu dostupne normalnom Android korisniku. Ove radnje uključuju deinstaliranje podrazumevanih aplikacija (naročito bloatvare) koje dolaze uz telefon. Rutovanje se takođe radi za ekstremno prilagođavanje; na primer, novi prilagođeni ROM-ovi se mogu preuzeti i instalirati. Međutim, sa tačke gledišta forenzičke analize, glavni razlog za rutovanje je dobijanje pristupa onim delovima sistema koji obično nisu dostupni. Većina javnih root alata će rezultirati stalnim root-om, gde promene traju čak i nakon ponovnog pokretanja uređaja. U slučaju privremenog root-a, promene se gube kada se uređaj ponovo pokrene. U forenzičkim slučajevima uvek treba dati prednost privremenim korenima.

Privatni podaci svake aplikacije se čuvaju na lokaciji ***/data/data*** i dostupni su samo toj aplikaciji. Dakle, tokom istrage nije moguće pristupiti podacima koji se nalaze na ovoj lokaciji. Međutim, rutovanje telefona će vam omogućiti pristup podacima prisutnim na bilo kojoj lokaciji. Važno je imati na umu da rutovanje telefona ima nekoliko implikacija, kao što je ovde opisano:

* **Bezbednosni rizik:** Rootiranje telefona može izložiti uređaj bezbednosnim rizicima. Na primer, zamislite zlonamernu aplikaciju koja ima pristup celom operativnom sistemu i podacima svih drugih aplikacija instaliranih na uređaju.
* **Zazidanje vašeg uređaja**: Ako rutovanje nije obavljeno na pravilan način, to može dovesti do kvara vašeg uređaja. "Bricking" je reč koja se obično koristi za telefone koji su mrtvi ili se ne mogu uključiti ni na koji način.
* **Poništavanje vaše garancije**: U zavisnosti od proizvođača i operatera, rutovanje uređaja može poništiti vašu garanciju, jer izlaže uređaj nekoliko pretnji.
* **Forenzičke implikacije**: Rutovanje Android uređaja će omogućiti istražitelju da pristupi većem skupu podataka, ali uključuje izmenu određenih delova uređaja. Dakle, uređaj treba da se rutuje samo kada je to apsolutno neophodno.

**Recovery mod**

Android telefon se može posmatrati kao uređaj koji ima tri glavne particije: pokretač, Android ROM i oporavak. Boot loader je prisutan na prvoj particiji i prvi je program koji se pokreće kada je telefon uključen. Primarni zadatak ovog pokretača je da se pobrine za inicijalizaciju hardvera niskog nivoa i pokrene uređaj na druge particije. Obično podrazumevano učitava Android particiju, koja se obično naziva Android ROM. Android ROM sadrži sve datoteke operativnog sistema koje su neophodne za pokretanje uređaja. Particija za oporavak, koja se obično naziva stock recoveri, je ona koja se koristi za brisanje svih korisničkih podataka i datoteka ili za ažuriranje sistema.

**Pristup recovery modu**

Recovery image se čuva na particiji za oporavak i sastoji se od Linux image sa jednostavnim korisničkim interfejsom koji se kontroliše pomoću hardverskih dugmadi. Režimu oporavka se može pristupiti na dva načina:

* Pritiskom na određene kombinacije tastera prilikom pokretanja uređaja (obično, držanjem tastera za jačinu zvuka +, jačinu zvuka - i za napajanje tokom pokretanja)
* Izdavanjem *adb reboot recovery* komande za pokrenut Android sistem

##### **Prilagodjen recovery**

Prilagođeni oporavak je okruženje za oporavak treće strane (third party). Flešovanje ovog okruženja za oporavak na vaš uređaj zamenjuje podrazumevano okruženje za oporavak sa prilagođenim okruženjem za oporavak treće strane. Ovo su najčešće funkcije koje su uključene u prilagođeni oporavak:

• Funkcija pune rezervne kopije i vraćanja (kao što je NANDroid)

• Dozvolite nepotpisane pakete ažuriranja ili dozvolite potpisane pakete sa prilagođenim ključevima

• Selektivno montira particije uređaja i SD karticu

• Omogućite pristup USB memoriji za SD karticu ili particije podataka

• Obezbedite pun pristup ADB-u, sa ADB demonom koji radi kao root

**Fastboot mod**

Fastboot je protokol koji se može koristiti za ponovno flešovanje particija na uređaju. To je jedan od alata koji dolazi uz Android SDK. To je alternativa režimu oporavka za instaliranje i ažuriranje, kao i za otključavanje pokretača u nekim slučajevima. Dok ste u fastboot mod-u, možete da menjate slike sistema datoteka sa računara preko USB veze. Dakle, to je jedan od načina za instaliranje slika za oporavak i samo pokretanje u nekim slučajevima. Kada se telefon pokrene u brzom pokretanju, možete flešovati datoteke slika u internoj memoriji. Na primer, prilagođene slike za oporavak, kao što je ClockvorkMod recovery mogu se flešovati na ovaj način.

**Zaključani i otključani boot loader-i**

Boot loaderi mogu biti zaključani ili otključani. Zaključani boot loaderi ne dozvoljavaju da izvršite modifikacije firmvera uređaja primenom ograničenja na nivou pokretača. Ovo se obično radi verifikacijom kriptografskog potpisa. Dakle, nepotpisani kod se ne može prebaciti na uređaj. Drugim rečima, da biste pokrenuli bilo koju sliku za oporavak ili sopstveni operativni sistem, prvo morate da otključate pokretač. Otključavanje pokretača može dovesti do ozbiljnih bezbednosnih implikacija.

Ako je uređaj izgubljen ili ukraden, napadač može da povrati sve podatke na njemu jednostavnim otpremanjem prilagođene slike za pokretanje Android-a ili flešovanjem prilagođene slike za oporavak. Dakle, napadač ima pun pristup podacima koji se nalaze na uređaju. Kao rezultat toga, vraćanje na fabrička podešavanja se vrši na telefonu prilikom otključavanja zaključanog pokretača tako da se svi podaci brišu. Stoga je važno da se ovo uradi samo kada je to apsolutno neophodno. Neki uređaji imaju načine da ih zvanično otključaju. Za ove uređaje, pokretač se može otključati stavljanjem uređaja u režim brzog pokretanja i pokretanjem komande *fast oem unlock*. Ovo će otključati pokretač i potpuno obrisati Android uređaj.

### **Razumevanje prostora za podatke na Androidu**

**Zajednicke particije na Androidu**

Izgled particije varira između proizvođača i verzija. Međutim, nekoliko particija je prisutno na svim Android uređajima. Sledeći odeljci objašnjavaju neke od uobičajenih particija koje se nalaze u većini Android uređaja.

***boot loader***

Ova particija skladišti program za pokretanje telefona. Ovaj program vodi računa o inicijalizaciji hardvera niskog nivoa kada se telefon pokrene. Dakle, on je odgovoran za pokretanje Android kernela i pokretanje u drugim režimima pokretanja, kao što su režim oporavka, režim preuzimanja i tako dalje.

***boot***

*Ova* particija ima informacije i datoteke potrebne za pokretanje telefona. Sadrži kernel i RAM disk. Dakle, bez ove particije, telefon ne može da pokrene svoje procese.

***recovery***

Particija za oporavak omogućava uređaju da se pokrene sa konzole za oporavak preko koje se obavljaju aktivnosti kao što su ažuriranja telefona i druge operacije održavanja. U tu svrhu se čuva minimalna slika za pokretanje Android-a. Ova slika za pokretanje služi kao zaštita od greške.

**userdata**

Ova particija se obično naziva particijom podataka i predstavlja internu memoriju uređaja za podatke aplikacije. Ovde se čuva veliki deo korisničkih podataka i tu će se nalaziti većina naših forenzičkih dokaza. Takođe čuva sve podatke aplikacije i standardne komunikacije.

***System***

Ovde su prisutne sve glavne komponente osim kernela i RAM diska. Slika Android sistema ovde sadrži Android okvir, biblioteke, sistemske binarne datoteke i unapred instalirane aplikacije. Bez ove particije, uređaj ne može da se pokrene u normalnom režimu.

***cache***

Ova particija se koristi za skladištenje podataka kojima se često pristupa i raznih drugih datoteka, kao što su evidencije oporavka i paketi ažuriranja preuzeti preko mobilne mreže.

***radio***

Uređaji sa mogućnostima telefonije imaju sliku osnovnog opsega sačuvanu u ovoj particiji koja vodi računa o različitim telefonskim aktivnostima.

**Hijerarhija fajlova**

******Da biste izvršili forenzičku analizu na bilo kom sistemu (desktop ili mobilni), važno je razumeti osnovnu hijerarhiju datoteka. Osnovno razumevanje toga kako Android organizuje svoje podatke u datoteke i fascikle pomaže forenzičkom analitičaru da suzi svoje istraživanje na određene lokacije. Ako ste upoznati sa sistemima sličnim Unix-u, vrlo dobro ćete razumeti hijerarhiju datoteka u Androidu. U Linux-u, hijerarhija datoteka je jedno stablo, pri čemu je vrh stabla označen kao /. Ovo se zove koren (root). Ovo se razlikuje od koncepta organizovanja datoteka u disk jedinicama (kao kod Windows-a). Bez obzira da li je sistem datoteka lokalni ili udaljeni, biće prisutan ispod korena. Android hijerarhija datoteka je prilagođena verzija ove postojeće Linux hijerarhije. Na osnovu proizvođača uređaja i osnovne Linux verzije, struktura ove hijerarhije može imati nekoliko beznačajnih promena. Da biste videli kompletnu hijerarhiju datoteka, morate imati root pristup. Sledeći snimak ekrana prikazuje hijerarhiju datoteka na Android uređaju:

***cache***

Ovo je direktorijum (/cache) gde Android skladišti podatke i komponente aplikacije kojima se često pristupa. Brisanje keša ne utiče na vaše lične podatke, već jednostavno briše postojeće podatke. Takođe postoji još jedan direktorijum u ovoj fascikli koji se zove lost+found. Ovaj direktorijum sadrži oporavljene datoteke (ako ih ima) u slučaju oštećenja sistema datoteka, kao što je pogrešno uklanjanje SD kartice bez demontaže i tako dalje. Keš može da sadrži forenzički relevantne artefakte, kao što su slike, istorija pregledanja i drugi podaci aplikacije.

***d***

Ovo je simbolična veza ka */sys/kernel/debug*. Ova fascikla se koristi za montiranje debugfs sistema datoteka i za otklanjanje grešaka kernela.

***data***

Ovo je particija koja sadrži podatke svake aplikacije. Većina podataka koji pripadaju korisniku, kao što su kontakti, SMS, birani brojevi i tako dalje, čuva se u ovoj fascikli. Ovaj folder ima značajan značaj sa forenzičke tačke gledišta jer sadrži vredne podatke.

***dalvik-cache***

Android aplikacije sadrže .dex datoteke koje su optimizovane verzije Java bytecode. Kada se aplikacija instalira na Android uređaju, neke modifikacije se vrše na odgovarajućoj .dex datoteci i kreira se rezultujuća datoteka pod nazivom *.odex* datoteka (optimizovana .dex datoteka). Zatim se kešuje u direktorijum */data/dalvik-cache* tako da ne mora da obavlja proces optimizacije svaki put kada učita *application.log.*

Ova fascikla sadrži nekoliko evidencija koje mogu biti korisne tokom ispitivanja, u zavisnosti od osnovnih zahteva.

***data***

Particija */data/data* sadrži privatne podatke svih aplikacija. Većina podataka koji pripadaju korisniku se čuva u ovoj fascikli. Ovaj folder ima značajan značaj sa forenzičke tačke gledišta jer sadrži vredne podatke

***dev***

Ovaj direktorijum sadrži posebne datoteke uređaja za sve uređaje. Ovo je tačka montiranja za *tempfs* sistem datoteka. Ovaj sistem datoteka definiše uređaje dostupne aplikacijama.

***init***

Prilikom pokretanja Android kernela, init program se izvršava. Ovaj program je prisutan u ovoj fascikli

***mnt***

Ovaj direktorijum služi kao tačka montiranja za sve sisteme datoteka, interne i eksterne SD kartice...

***proc***

Ovo je tačka montiranja za procfs sistem datoteka koja obezbeđuje pristup strukturama podataka kernela. Nekoliko programa koristi */proc* kao izvor informacija. Sadrži datoteke koje sadrže korisne informacije o procesima.

***root***

Ovo je početni direktorijum za root nalog. Ovoj fascikli se može pristupiti samo ako je uređaj rootovan

***sbin***

Ovo sadrži binarne datoteke za nekoliko važnih daemona. Ovo nije od velikog značaja iz forenzičke perspektive

***misc***

Kao što ime sugeriše, ova fascikla sadrži informacije o raznim podešavanjima. Ova podešavanja uglavnom definišu stanje, odnosno UKLJUČENO/ISKLJUČENO. Iz ove fascikle može se pristupiti informacijama o postavkama hardvera, USB podešavanjima itd

***sdcard***

Ovo je particija koja sadrži podatke prisutne na SD kartici uređaja. SD kartica može biti ili prenosiva memorija ili memorija koja se ne može ukloniti. Svaka aplikacija na telefonu sa dozvolom *WRITE\_EXTERNAL\_STORAGE* može da kreira datoteke ili fascikle na ovoj lokaciji. Postoje neke podrazumevane fascikle, kao što su *android\_secure, Android, DCIM, media* i tako dalje, prisutne u većini mobilnih telefona.

Slike digitalnog fotoaparata (*DCIM*) je podrazumevana struktura direktorijuma za digitalne kamere, pametne telefone, tablete i srodne SSD uređaje. Neki tableti imaju fasciklu sa fotografijama koja pokazuje na istu lokaciju. U okviru DCIM-a ćete pronaći fotografije koje ste snimili, video zapise i sličice (keš) datoteke. Fotografije se čuvaju u */DCIM/Camera.*

***system***

Ovaj direktorijum sadrži biblioteke, sistemske binarne datoteke i druge sistemske datoteke. Unapred instalirane aplikacije koje dolaze uz telefon su takođe prisutne na ovoj particiji

***build.prop***

Ova datoteka sadrži sva svojstva build i podešavanja za dati uređaj. Za forenzičkog analitičara, ova datoteka daje pregled o modelu uređaja, proizvođaču, verziji Android-a i mnogim drugim detaljima.

***app***

Ovaj folder sadrži sistemske aplikacije i unapred instalirane aplikacije. Ovo je montirano kao samo za čitanje da bi se sprečile bilo kakve promene.

***framework***

Ova fascikla sadrži izvore za Android framework. U ovoj particiji možete pronaći implementaciju ključnih usluga, kao što je sistemski server sa menadžerima paketa i aktivnosti. Ovde se takođe radi mnogo mapiranja između API-ja Java aplikacije i izvornih biblioteka.

Podaci koji pripadaju različitim aplikacijama mogu se čuvati interno ili eksterno. U slučaju eksterne memorije (SD kartice), podaci se mogu čuvati na bilo kojoj lokaciji. Međutim, u slučaju interne memorije, lokacija je unapred definisana. Interni podaci svih aplikacija prisutnih na uređaju (bilo sistemskih aplikacija ili aplikacija koje su instalirali korisnici) automatski se čuvaju u poddirektorijumu */data/data*, nazvanom po imenu paketa.

Android pruža programerima određene opcije za čuvanje podataka na uređaju. Opcija koja se može koristiti zavisi od osnovnih podataka koji se čuvaju. Podaci koji pripadaju aplikacijama mogu se čuvati na jednoj od sledećih lokacija:

* Shared preferences
* Internal storage
* External storage
* SQLite database
* Network

**Shared preferences**

Ova lokacija pruža framework za čuvanje parova ključ-vrednost primitivnih tipova podataka u *.xml* formatu. Primitivni tipovi podataka uključuju boolean, float, int, long i string. Nizovi se čuvaju u formatu UTF-8. Ove datoteke se obično čuvaju na */data/data/<package\_name>/shared\_prefs* putanji aplikacije. Na primer, folder *shared\_prefs* za Android aplikaciju za e-poštu sadrži manje od šest *.xml* datoteka,

**Internal storage**

Datoteke ovde se čuvaju u internoj memoriji. Ove datoteke se obično nalaze u poddirektorijumu */data/data* aplikacije. Podaci sačuvani ovde su privatni i ne mogu im pristupiti druge aplikacije. Čak je i vlasnik uređaja sprečen da pregleda datoteke (osim ako nemaju root pristup). Međutim, na osnovu zahteva, programer može dozvoliti drugim procesima da modifikuju i ažuriraju ove datoteke.

**External storage**

Datoteke takođe mogu da čuvaju aplikacije u spoljnoj memoriji. Eksterna memorija može biti prenosivi medij, kao što je SD kartica ili memorija koja se ne može ukloniti koja dolazi uz telefon. U slučaju uklonjive SD kartice, podaci se mogu koristiti na drugim uređajima samo uklanjanjem SD kartice i umetanjem u bilo koji drugi uređaj. SD kartice se obično formatiraju sa FAT32 sistemom datoteka, ali se i drugi sistemi datoteka, kao što su EXT3 i EXT4, takođe sve više koriste. Za razliku od interne memorije, eksterna memorija nema stroge mere bezbednosti. Podaci koji su ovde uskladišteni su javni i mogu im pristupiti druge aplikacije, pod uslovom da aplikacije koje zahtevaju imaju potrebne dozvole.

**SQLite database**

SQLite je popularan format baze podataka prisutan u mnogim mobilnim sistemima i koristi se za skladištenje strukturiranih podataka. SQLite je otvorenog koda i za razliku od mnogih drugih baza podataka, kompaktan je i nudi mnogo funkcionalnosti. Android podržava SQLite preko namenskih API-ja, i stoga programeri to mogu da iskoriste. SQLite baze podataka su bogat izvor forenzičkih podataka. SQLite datoteke koje koriste aplikacije uglavnom se čuvaju u */data/data/<ApplicationPackageName>/databases*. Sa forenzičke tačke gledišta, oni su veoma vredni jer često čuvaju mnogo važnih podataka kojima aplikacija rukuje.

**Network**

Možete da koristite mrežu za skladištenje i preuzimanje podataka na sopstvenim web uslugama. Za obavljanje mrežnih operacija mogu se koristiti klase u paketima *java.net.\** i *android.net.\**. Ovi paketi obezbeđuju programerima API-je niskog nivoa koji su neophodni za interakciju sa mrežom, web serverima.

**Generalni pregled Android fajl sistema**

Razumevanje sistema datoteka je veoma važno u Android forenzici, jer nam pomaže da steknemo znanje o tome kako se podaci čuvaju i preuzimaju. Ovo znanje o svojstvima i strukturi sistema datoteka će se pokazati korisnim tokom forenzičke analize. Sistem datoteka se odnosi na način na koji se podaci čuvaju, organizuju i preuzimaju. Osnovna instalacija može biti zasnovana na jednom volumenu podeljenom na nekoliko particija, ovde, svakom particijom može upravljati drugačiji sistem datoteka. Korisnici Microsoft Windows-a uglavnom su upoznati sa sistemom datoteka FAT32 ili NTFS, dok su korisnici Linux-a više upoznati sa EXT2 ili EXT4 sistemom datoteka. Kao što je tačno u Linux-u, Android takođe koristi tačke montiranja, a ne diskove (to je C: ili E:). Svaki sistem datoteka definiše svoja pravila za upravljanje datotekama na volumenu. U zavisnosti od ovih pravila, svaki sistem datoteka nudi različitu brzinu za preuzimanje datoteka, bezbednost, veličinu itd. Linux koristi nekoliko sistema datoteka, kao i Android. Sa forenzičke tačke gledišta, važno je razumeti koje sisteme datoteka koristi Android i identifikovati sisteme datoteka koji su od značaja za istragu. Na primer, sistem datoteka koji skladišti podatke korisnika je od primarnog značaja za nas, za razliku od sistema datoteka koji se koristi za pokretanje uređaja.

Poznato je da Linuk podržava veliki broj sistema datoteka. Ovim sistemima datoteka koje koristi sistem ne pristupa se preko imena disk jedinica, već se umesto toga kombinuju u jednu hijerarhijsku strukturu stabla koja predstavlja ove sisteme datoteka kao jedan entitet. Svaki novi sistem datoteka se dodaje u ovo jedno stablo sistema datoteka kada se montira.

**Logička ekstrakcija podataka**

U tradicionalnoj kompjuterskoj forenzici, logičko izdvajanje je analogno kopiranju i lepljenju fascikle u cilju izdvajanja podataka iz sistema, ovaj proces će kopirati samo datoteke kojima korisnik može pristupiti i videti. Ako su skrivene ili izbrisane datoteke prisutne u fascikli koja se kopira, one neće biti u nalepljenoj verziji fascikle.

Granica između logičke i fizičke ekstrakcije u mobilnoj forenzici je nešto nejasnija nego tradicionalnoj kompjuterskoj forenzici. Na primer, izbrisani podaci se rutinski mogu oporaviti iz logičkih ekstrakcija na mobilnim uređajima, zbog rasprostranjenosti SQLite baza podataka koje se koriste za skladištenje podataka.Skoro svaka mobilna ekstrakcija će zahtevati neki oblik interakcije sa Android operativnim sistemom, nema jednostavnog ekvivalenta izvlačenju čvrstog diska i snimanju istog bez pokretanja diska. Definisaćemo logičko izdvajanje kao proces koji dobija podatke vidljive korisniku, a može uključivati podatke koji su označeni za brisanje.

**Sta moze da se spasi?**

Uglavnom, svi i svi korisnički podaci mogu se logički povratiti:

* Kontakti
* Evidencije poziva
* SMS/MMS
* Informacije o alpikaciji
* Sistemske evidencije i informacije

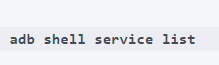
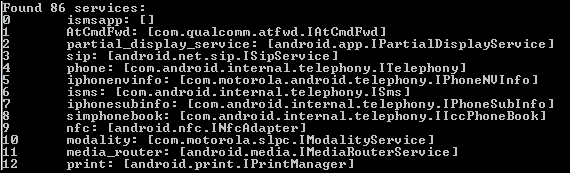
Bez root pristupa, forenzički ispitivač ne može jednostavno kopirati informacije sa particije podataka. Ispitivač će morati da pronađe neki metod za eskalaciju svojih privilegija kako bi dobio pristup kontaktima, evidenciji poziva, SMS/MMS-u i podacima aplikacije. Ove metode često nose mnoge rizike, kao što je mogućnost da unište ili „pokvare“ uređaj (što ga čini nemogućim da se pokrene) i mogu izmeniti podatke na uređaju kako bi se postigao trajnost. Metode se obično razlikuju od uređaja do uređaja i ne postoji univerzalna metoda jednim klikom za dobijanje root pristupa svakom uređaju. Komercijalni mobilni forenzički alati kao što su **MicroSystemation XRY**  i **Cellebrite UFED**  imaju ugrađene mogućnosti za privremeno i bezbedno rutovanje mnogih uređaja, ali ne pokrivaju širok spektar svih Android uređaja.

**Ručna ADB ekstrakcija**

ADB *pull* komanda se može koristiti za povlačenje pojedinačnih datoteka ili čitavih direktorijuma direktno sa uređaja na računar forenzičkog ispitivača. Ova metoda je posebno korisna za male, ciljane preglede. Na primer, u istrazi koja striktno uključuje SMS poruke, ispitivač može izabrati da izvuče samo relevantne datoteke.

**ADB Dumpsys**

**Dumpsis je alatka ugrađena u Android OS, koja se uglavnom koristi u razvojne svrhe da bi se prikazao status usluga koje rade na uređaju. Međutim, može da sadrži i forenzički zanimljive informacije. Dumpsis ne zahteva root pristup, ali kao i sve ADB komande, zahteva da se USB otklanjanje grešaka omogući na uređaju i da se zaobiđe bezbedno USB otklanjanje grešaka.**

**Tačne usluge koje se mogu videti razlikuju se na različitim uređajima i verzijama Android-a. Da biste videli listu svih mogućih usluga koje se mogu izbaciti, pokrenite sledeću komandu:**

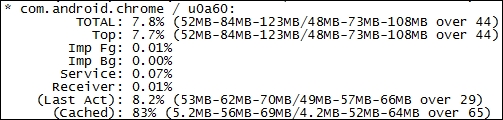
**Izlaz *service list* komande**

**Dumpsys batterystats**

Batteristats se koristi za prikaz upotrebe pokrenutih aplikacija. Njegov izlaz može biti veoma opsežan, u zavisnosti od broja aplikacija koje se koriste.

Ovo nam pokazuje upotrebu mreže Google Chrome-a. Ove informacije se mogu koristiti da bi se pokazalo da je aplikacija nedavno korišćena, a ove informacije će postojati čak i ako je Chrome korišćen u anonimnom režimu i ne ostavlja forenzičke dokaze na drugom mestu.

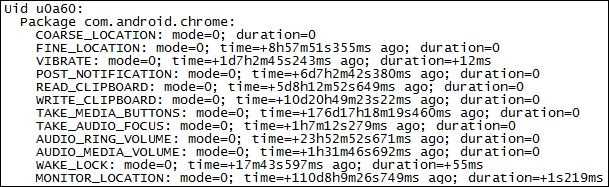
**Dumpsys procstats**

**Procstats** je usluga za prikaz upotrebe procesora pokretanjem aplikacija. Slično statistici baterije, to je još jedan metod koji se može koristiti da se pokaže da je aplikacija nedavno korišćena na uređaju, kao što je prikazano na sledećem snimku ekrana:

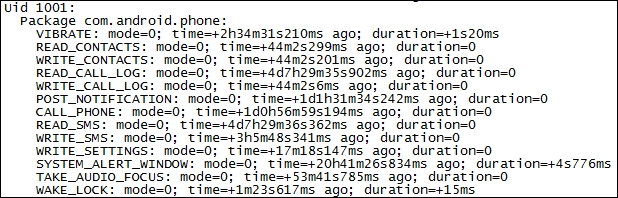
**Dumpsys user**

Počevši od Android Jelli Bean-a, Google je dodao podršku za više korisnika na tablet uređajima. Sa izdavanjem Lollipop-a, Google je proširio ovu podršku na telefone. Jedan od najizazovnijih problema u digitalnoj forenzici dugo vremena je bio da se dokaže ko je koristio uređaj kada su izvršene inkriminišuće radnje; „Ko je bio iza tastature?“

**Dumpsys App Ops**

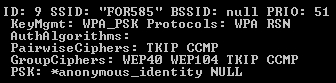
App Ops je najzanimljivija dumpsys usluga. Termin App Ops se generalno koristi za označavanje dozvola kojima aplikacija pristupa. U starijim verzijama Android-a, pričalo se da će Google uključiti mogućnost da korisnici povuku određene dozvole iz aplikacije. Ovo se nikada nije ostvarilo, ali ova usluga barem ostaje i pokazuje kada je aplikacija poslednji put koristila svaku dozvolu kojoj može da pristupi. Sledi još jedan primer iz Google Chrome-a:

U gornjem izlazu, možemo videti da je otprilike 1 sat i 7 minuta pre nego što je App Ops bačen pomoću dumpsis-a, Chrome koristio dozvolu **TAKE\_AUDIO\_FOCUS**, a kasnije koristio **AUDIO\_MEDIA\_VOLUME**. Ovo pokazuje šta je Chrome korišćen za slušanje i kada.

Nešto zanimljiviji primer je sledeća telefonska aplikacija

Pre 44 minuta, korisnik je koristio telefonsku aplikaciju i zahtevao je dozvolu READ\_CONTACTS, a zatim je odmah koristio dozvolu WRITE\_CALL\_LOG. Možemo pretpostaviti da je korisnik telefonirao pre 44 minuta, čak i da su posle izbrisali poziv iz evidencije.

**Dumpsys Wi-Fi**

**Wi-F** usluga će prikazati listu svih SSID-ova za koje je veza sačuvana. Ovo bi moglo biti korisno za pokazivanje da je korisnik bio na određenoj lokaciji, na primer. Detaljnije informacije o Wi-Fi-ju su takođe dostupne u sistemu datoteka, ali za pregled je potreban root. Koristeći dumpsis, možemo pristupiti ovim podacima bez potrebe za root-om:

**Zaobilaženje Android ekrana za zaključavanje**

Zaključani ekrani su najizazovniji aspekt Android forenzičkih ispitivanja. Često cela istraga zavisi od sposobnosti ispitivača da pristupi zaključanom uređaju. Iako postoje metode da ih se zaobiđe, to može u velikoj meri zavisiti od verzije OS-a, podešavanja uređaja i tehničkih mogućnosti ispitivača. Ne postoji magično rešenje koje će raditi svaki put na svakom uređaju. Komercijalni forenzički alati kao što su Cellebrite i XRY imaju prilično robusne mogućnosti zaobilaženja, ali su daleko od nepogrešivih. Ovo poglavlje će pokazati kako ispitivač može povećati svoje šanse da zaobiđe zaključane uređaje pomoću besplatnih alata i metoda.

**Tipovi ekrana za zakljucavanje**

Postoji mnogo metoda koje se koriste za osiguranje uređaja, a metode za zaobilaženje se razlikuju:

* Ništa/Slide
* Šablon
* PIN
* Lozinka
* Smart Lock

**Generalne informacije**

U svim slučajevima, zaobilaženje zaključanog ekrana zahtevaće preuzimanje datoteke sa uređaja. Zaključavanja šablona se čuvaju kao heš vrednosti na */data/sistem/gesture.key*, a zaključavanja PIN-om/lozinkom se čuvaju kao heš vrednosti na /data/sistem/passvord.kei. Dodatno, heš passvord.key je “soljen“ (salted), vrednost soli se čuva u */data/data/com.android.providers.settings/databases/settings.db* pre Androida 4.4 i /data/sistem/locksettings.db na uređajima koji koriste Android 4.4 i novije verzije.

Fajlovi koje treba povući da bi se razbio PIN/lozinka na uređajima pre Android 4.4 su:

* /data/system/password.key
* /data/data/com.android.providers.settings/databases/settings.db

Fajlovi koje treba povući da bi se razbio PIN/lozinka na uređajima koji koriste Android 4.4 i novije verzije su:

* /data/system/password.key
* /data/system/locksettings.db

Potrebno je povući samo jednu datoteku da biste razbili Pattern lock na svim verzijama Android-a:

* /data/system/gesture.key

**Razbijanje sifre**

Sada kada imamo **gesture.key**, koji sadrži informacije o zaključavanju šablona, pogledajmo sadržaj datoteke:

Heksadecimalni sadržaj datoteke je neslani SHA-1 heš šablona prevlačenja. Činjenica da postoji ograničen broj mogućih obrazaca (postoji minimum od četiri cifre i maksimum od devet cifara jer se svaki broj može koristiti samo jednom), najjednostavniji metod za razbijanje ovog heša je napad iz rečnika. Ispitivač može da napravi rečnik koji se sastoji od svih mogućih obrazaca, ali ponovno izmišljanje točka nije uvek neophodno.

**Fizicka ekstrakcija podataka**

**Pregled fizicke ekstrakcije**

U digitalnoj forenzici, fizička ekstrakcija je tačna bit-za-bit slika elektronskog medija, a ova definicija ostaje tačna i za mobilne uređaje. U tradicionalnoj kompjuterskoj forenzici, ovo obično uključuje uklanjanje diska sa dokazima sa računara osumnjičenog i njegovo snimanje putem blokade pisanja bez pokretanja disk jedinice, što rezultira datotekom slike koja sadrži tačnu kopiju disk jedinice osumnjičenog. Izlaz se često naziva **neobrađena slika** ili jednostavno **bin** (binarna) datoteka. Fizička ekstrakcija se razlikuje od logičkog, po tome što su tačna kopija memorije uređaja i uključuju nedodeljeni prostor, zastoj fajlova, slabljenje jačine zvuka i tako dalje.

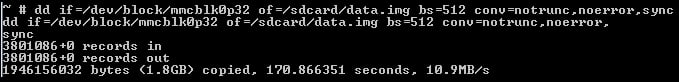
U mobilnoj forenzici rezultat je isti; tačnu bit-za-bit sliku uređaja, ali metode su nešto drugačije. Na primer, uklanjanje fleš memorije sa uređaja na sliku može biti i dugotrajno i skupo, i zahteva mnogo specijalizovanog znanja (iako se može uraditi kao što je objašnjeno u odeljku o odvajanju kasnije u poglavlju). Osim korišćenja napredne **Joint Test Action Group** (**JTAG**) ili metoda chip-off-a, uređaj mora biti pokrenut do određenog stepena (i upisan na njega u mnogim slučajevima) da bi pristupio podacima. Konačno, pronalaženje alata koji čak može da analizira konačnu datoteku slike može biti veoma teško. Slike čvrstog diska i sistemi datoteka su dugo dokumentovani i proučavani, dok se slike i sistemi datoteka za mobilne uređaje često menjaju. U nekim slučajevima mobilni sistemi datoteka su čak jedinstveni za određenog proizvođača. Znati šta raditi sa slikom nakon što je stečena može biti jednako izazovna kao i sticanje slike.

**Extracting data physically with dd**

Komanda ***dd*** bi trebalo da bude poznata svakom ispitivaču koji je radio tradicionalnu forenziku čvrstog diska. Komanda ***dd*** je Linux uslužni program komandne linije koji se po definiciji koristi za konvertovanje i kopiranje datoteka, ali se često koristi u forenzici za kreiranje detaljnih slika celih diskova. Mnoge varijacije dd komandi takođe postoje i obično se koriste, kao što su **dcfldd**, **dc3dd**, **ddrescue** i dd\_**rescue**. Pošto je komanda **dd** izgrađena za sisteme zasnovane na Linux-u, često je uključena na Android platformama. To znači da metoda za kreiranje slike uređaja često već postoji na uređaju.

Komanda **dd** ima mnogo opcija koje se mogu podesiti, od kojih su ovde navedene samo forenzički važne opcije. Format komande **dd** je sledeći

Nakon što odredite koji blok za čitanje i gde je SD kartica simbolički povezana, slikajte particiju /data na /sdcard, koristeći sledeću komandu:

Sada, slika /data particije postoji na SD kartici. Može se povući na mašinu ispitivača pomoću ADB pull komande ili jednostavno pročitati sa SD kartice. 

**Forenzička analiza aplikacija na uredjaju**

Forenzička analiza aplikacije je umetnost koliko i nauka. Postoji bezbroj načina na koje aplikacija može da skladišti ili prikriva svoje podatke. Različite verzije iste aplikacije mogu čak različito čuvati iste podatke. Programer je zaista ograničen samo svojom maštom (i ograničenjima Android platforme) kada je u pitanju izbor kako da čuva svoje podatke. Kao rezultat ovih faktora, analiza aplikacije je cilj koji se stalno menja. Metode koje ispitivač koristi jednog dana mogu biti potpuno irelevantne sledećeg.

**Gmail**

Direktorijum */cache* unutar fascikle aplikacije sadrži nedavne datoteke koje su priložene e-porukama, poslate i primljene. Ovi prilozi se čuvaju ovde čak i ako ih korisnik nije izričito preuzeo.

Datoteka *mailstore.<username>@gmail.com.db* sadrži niz korisnih informacija. Zanimljive tabele u bazi podataka uključuju sledeće:

Krajnji cilj forenzičke analize aplikacije je dosledno isti, da se razume za šta je aplikacija korišćena i da se pronađu korisnički podaci.

Baza *suggestions.db* sadrži termine koji su pretraživani unutar aplikacije.

XML datoteke unutar shared\_prefs direktorijuma mogu potvrditi nalog(e) koji su korišćeni sa aplikacijom. Gmail.xml je sadržao još jedan nalog koji je bio povezan sa našim probnim nalogom, ali nikada nije korišćen sa aplikacijom. UnifiedEmail.xml je sadržao delimičnu listu pošiljalaca koji su poslali e-poštu nalogu, ali bez vidljivog obrazloženja. Mnogi pošiljaoci su bili na listi, ali daleko od svih, i nisu se pojavljivali po nekom određenom redosledu. Gmail.xml je takođe sadržao poslednji put kada je aplikacija sinhronizovana u formatu Linux epohe.

**Facebook**

Direktorijum */files/video-cache* sadrži video zapise iz korisnikovog fida vesti, iako izgleda da ne postoji način da se oni povežu nazad sa korisnikom koji ih je postavio.

Direktorijum */cache/images* sadrži slike iz korisničkog fida vesti, kao i fotografije profila kontakata. Ovaj direktorijum sadrži mnoštvo drugih direktorijuma (65 na našem test telefonu), a svaki direktorijum može da sadrži više .cnt datoteka. .cnt datoteke su obično .jpg datoteke ili drugi formati slika.

Baza podataka *bookmarks\_db2* je lista stavki koje se pojavljuju na strani korisnikovog fida vesti, kao što su grupe i aplikacije. Mnoge od ovih obeleživača automatski generiše Facebook, ali ih može kreirati i korisnik.

Baza podataka *contacts\_db2* predvidljivo sadrži informacije o svim kontaktima korisnika

Baza podataka *nearbitiles\_db* sadrži lokacije u blizini korisnika koje bi ga mogle zanimati. Ovo je očigledno stalno popunjeno, čak i ako korisnik ne vidi lokacije. Zanimljivo je zato što, iako nije dobra lokacija (većina naših testova je pokazala lokacije unutar 6–10 milja od naše lokacije), to je gruba ideja o mestima na kojima je korisnik bio.

*newsfeed\_db* baza podataka sadrži podatke prikazane korisniku u njihovom newsfeedu. U zavisnosti od upotrebe aplikacije, to može biti veoma velika datoteka

**Viber**

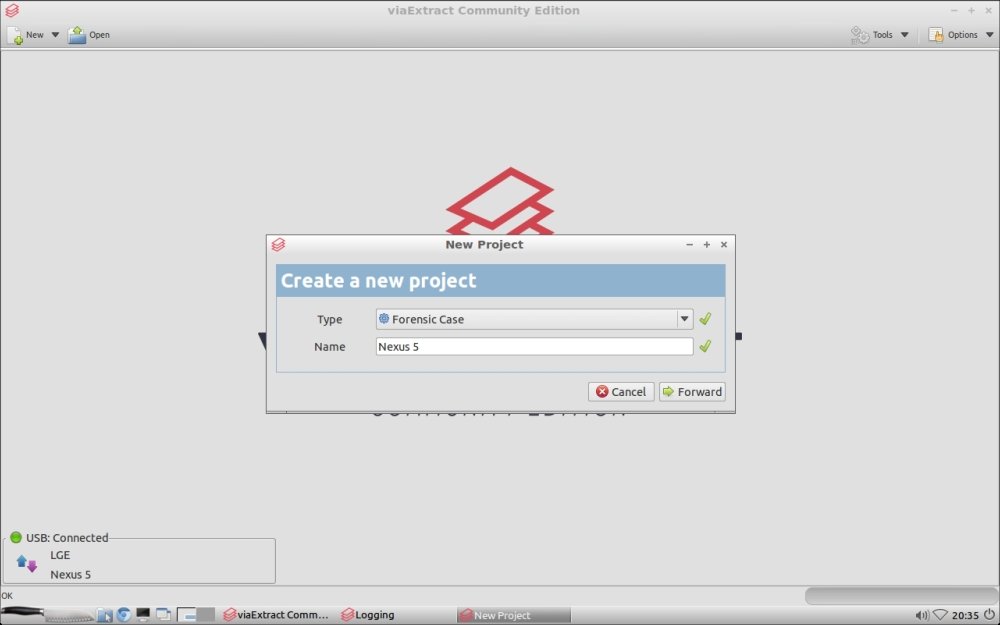
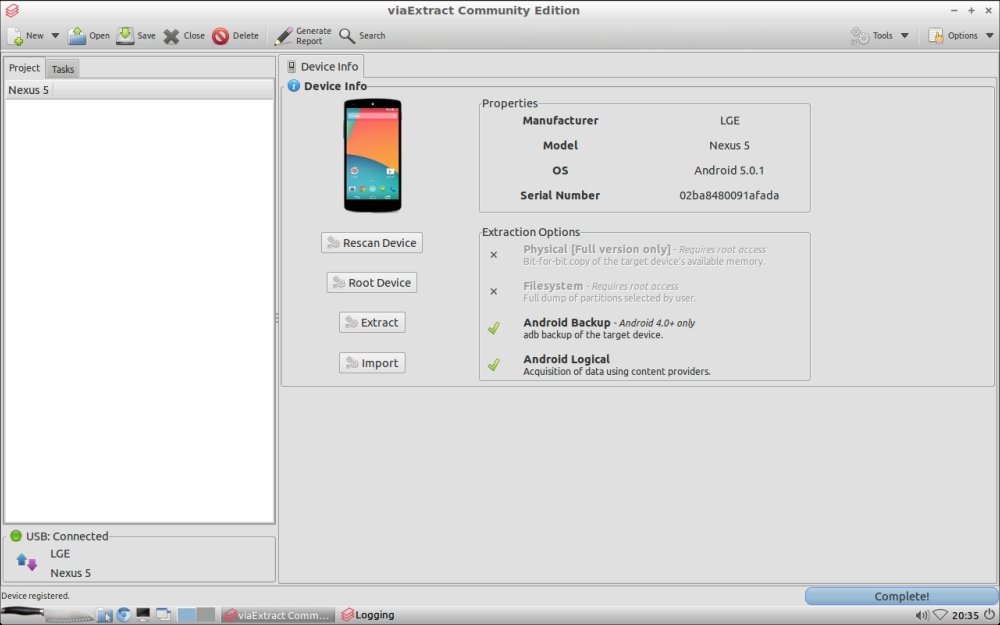
Datoteke u */files/preferences* sadrže ID kartice sa integrisanim kolom (ICCID) SIM kartice, ime koje korisnik prikazuje u aplikaciji i broj telefona koji se koristi za registraciju u aplikaciji.

Datoteke na */sdcard/viber/media* putanji su fotografije profila ljudi sa liste kontakata korisnika koji koriste Viber (bez obzira da li su dodani kao prijatelji u aplikaciji) i sve slike i video zapisi poslati preko aplikacije.

Datoteka *viber\_data* je baza podataka, iako nema ekstenziju datoteke .db. Sadrži informacije o kontaktima korisnika.

**Pregled gotovih alata iz ove oblasti**

ViaExtract

Registracija je obavezna. ViaExtract je logički i fizički alat za ekstrakciju kreiran od strane NowSecure (ranije poznat kao ViaForensics). Logičke akvizicije (uključujući rezervne kopije) dostupne su uz besplatnu verziju, dok plaćena verzija dodaje fizičke ekstrakcije. Slobodno se distribuira unutar datoteke virtuelne mašine (bilo formata VMVare ili Virtual Bok) koja pokreće NowSecure-ovu Santoku Linux distribuciju. Za korišćenje besplatne verzije potrebna je aktivna internet veza. Registracija je obavezna.

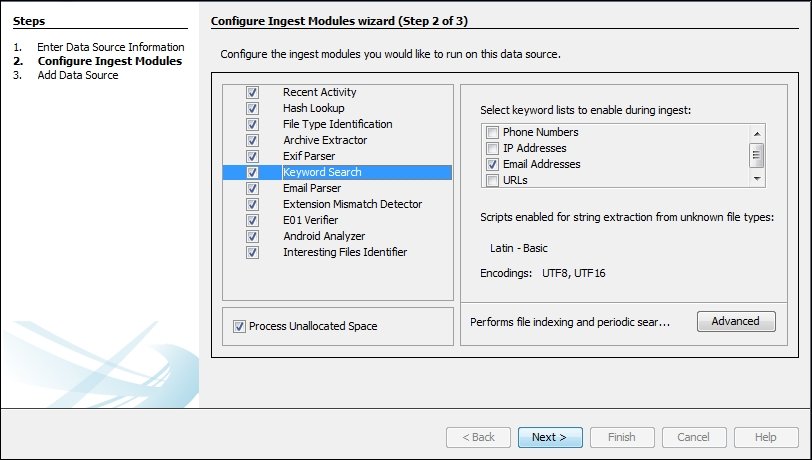
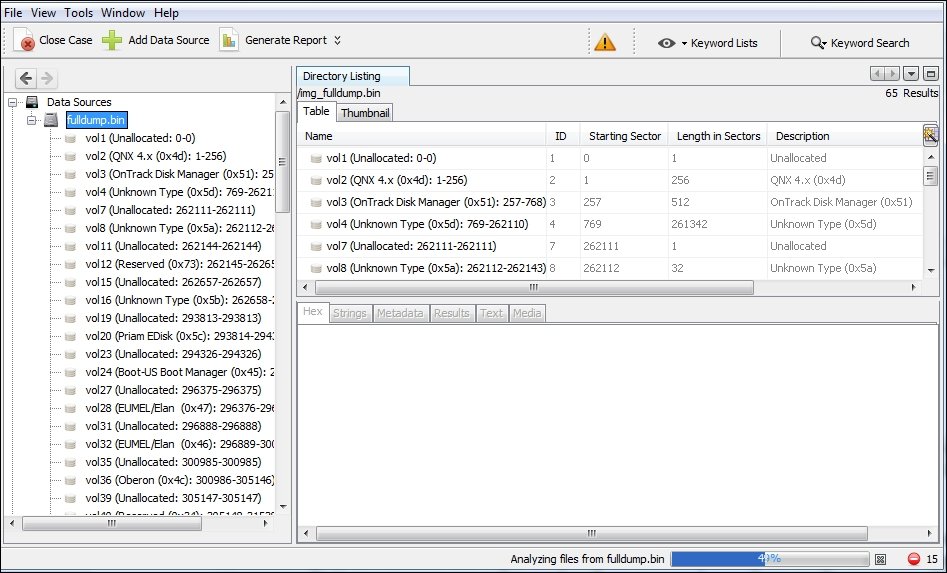
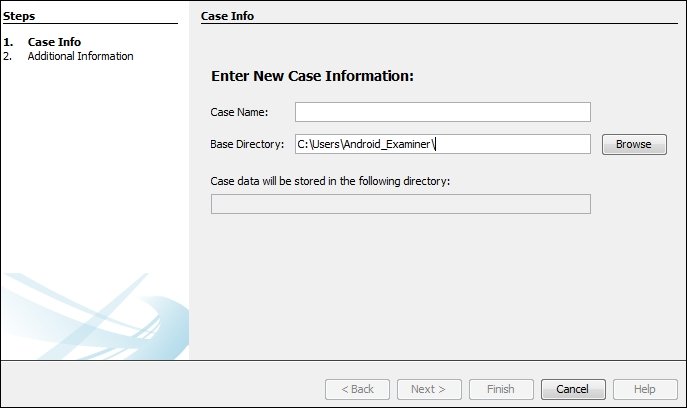
ViaExtract takođe može pokušati da iskoreni uređaj i zaobiđe šifru. Klikom na dugme Root na kartici Informacije o uređaju pokrenuće se wizard za rutovanje. Jednostavno pratite iskačuće poruke da biste root-ovali uređaj.

Wizard za obilazak zaključanog ekrana se pokreće iz menija Alatke u gornjem desnom uglu. Zatim izaberite Otključaj ekran. Ovo će gurnuti aplikaciju na uređaj (koja zahteva da se omogući otklanjanje grešaka na USB-u i da se prođe RSA autentifikacija) koja će ukloniti zaključani ekran. Ovo je korisna alatka jer ne zahteva root pristup. Nije uspešan na nekim uređajima kao što su Nekus 5 i HTC Droid DNK, ali savršeno radi Moto X.

Autopsy

Autopsy je besplatan alat za analizu otvorenog koda koji je prvobitno razvio Brian Carrier. Autopsy je počela kao grafički korisnički interfejs za osnovni set alata SleuthKit zasnovan na Linux-u, ali najnovije izdanje (verzija 3) je samostalna alatka napravljena za Windows.

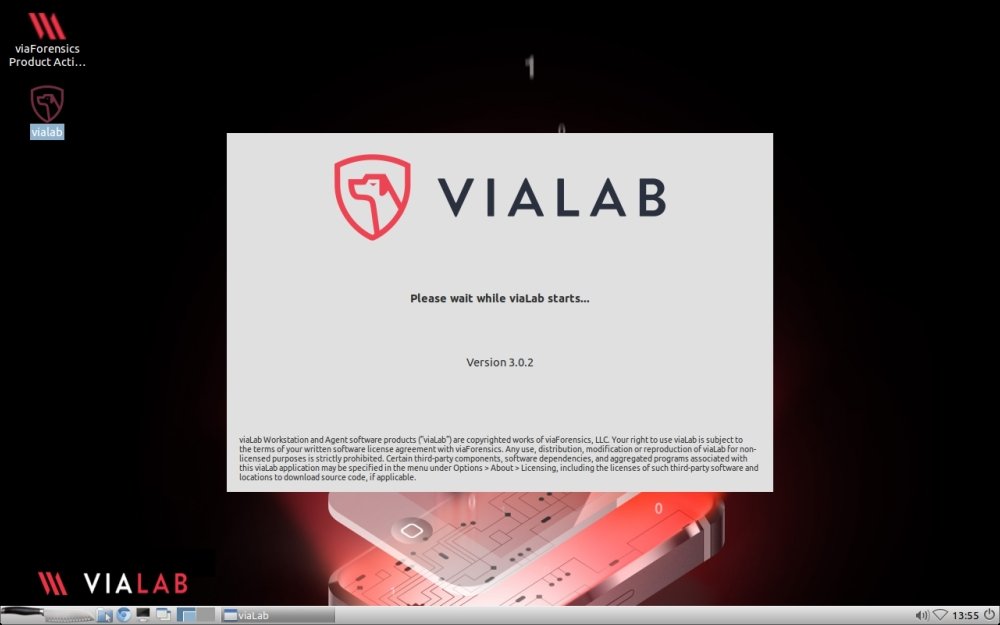
Autopsija nije namenjena za akviziciju mobilnih uređaja, ali može da analizira najčešće Android sisteme datoteka (kao što su YAFFS i ext).

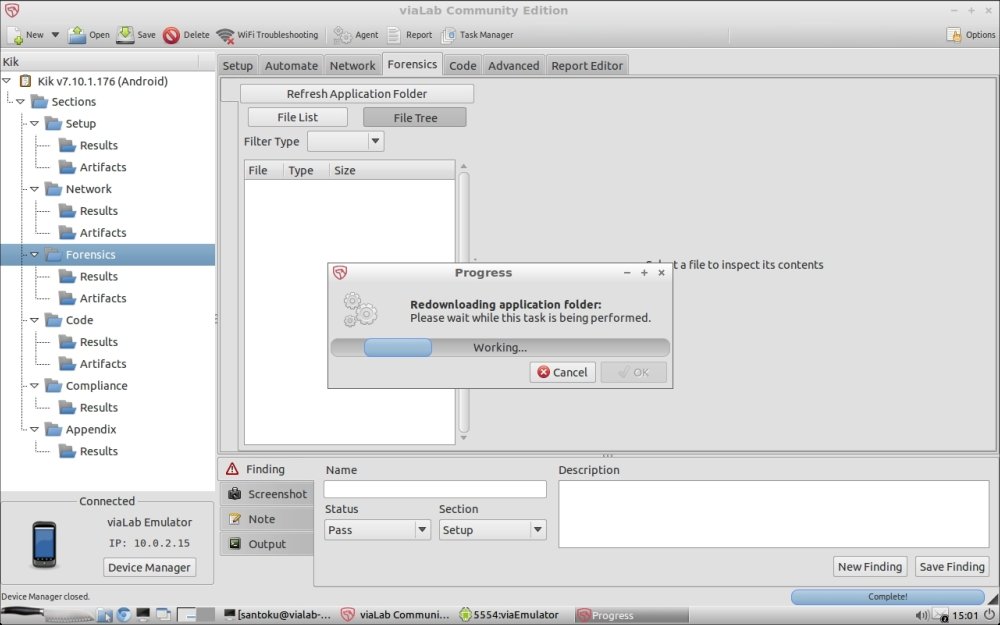
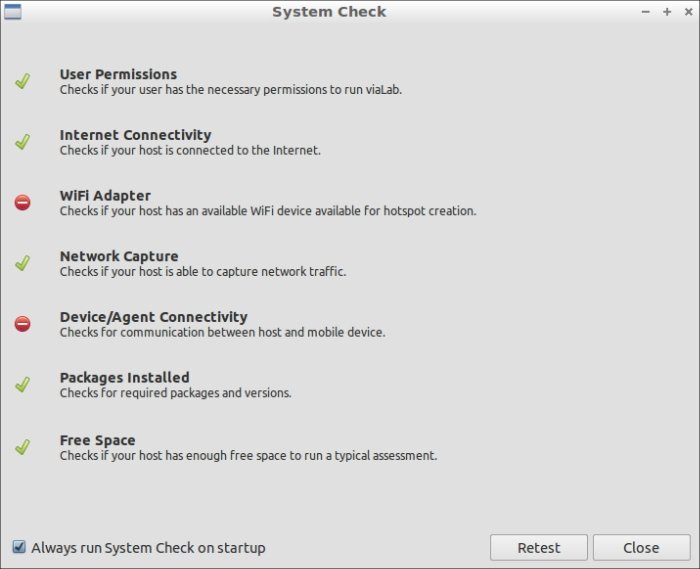


## ViaLab Community Edition

ViaLab Communiti Edition je još jedan besplatni alat koji je razvio i objavio NowSecure. Isporučuje se kao samostalna virtuelna mašina. VM je zapravo veoma sličan preuzimanju sa Santokua. ViaLab zahteva da računar ispitivača ima internet vezu, da bi koristio alat.

Glavna svrha ViaLab-a je da analizira ponašanje APK-a, iako mnoge funkcije za to nisu dostupne u besplatnom izdanju zajednice. ViaLab vam omogućava da ručno učitate APK datoteku u Android emulator ili da pokrenete aplikaciju na root-ovanom uređaju. Dobar slučaj forenzičke upotrebe za ovo bi bio istraživanje aplikacije da biste saznali koje podatke čuva. Na primer, ako tužilac traži sačuvane video snimke, ispitivač može da utvrdi da li aplikacija ima tu mogućnost i gde se oni čuvaju.





|  |  |
| --- | --- |
| ViaExtract | * Besplatno, zahteva registraciju i aktivnu internet vezu * Logička ekstrakcija preko aplikacije koja je gurnuta na uređaj * Izvlačenje rezervnih kopija * Ekstrakcije sistema datoteka ako je uređaj ukorenjen * Root uređaji * Zaobilazi zaključavanje ekrana bez root-a guranjem aplikacije na uređaj |
| Autopsy | * Besplatan i otvoren izvor * Koristi se za ispitivanje ekstrakcija urađenih drugim alatima * Omogućava pretragu ključnih reči, heš liste i druge uobičajene forenzičke metode * Moćna funkcija vremenske linije * Može da povrati izbrisane podatke sa podržanih sistema datoteka |
| ViaLab | * Besplatno, zahteva registraciju i aktivnu internet vezu * Dozvoljava ispitivaču da pokrene aplikaciju iz APK-a i odredi lokacije za skladištenje podataka * Pokreće aplikaciju u emulatoru ili na uređaju za testiranje * Vredna alatka koja pokazuje ispitivaču gde se podaci čuvaju u direktorijumu aplikacije, kao i da vidi funkcionalnost aplikacije |

**Literatura**

Learning Android Forensics Rohit Tamma, Donnie Tindall

Android Forensic Acquisition Techniques | Medium članak Lucideus Forensics

Getting started with android forensics | članak Infosecintitute

Android phone forensic: Tools and techniques Conference | PDF 2016 International Conference on Computing Nihar Ranjan Roy, Anshul Kanchan Khanna, Leesha Aneja

Incident Response for Android and iOS | PDF NowSecure

Tools for carrying out forensic analyses on mobile devices | Blog incibe-cert