FORENZIKA MOBILNIH UREĐAJA

Matoić, Dragutin

Master's thesis / Specijalistički diplomski stručni

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:480169

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-20**

Repository / Repozitorij:

Algebra Univerity College - Repository of Algebra Univerity College

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

FORENZIKA MOBILNIH UREĐAJA

Dragutin Matoić

Zagreb, rujan 2019.

Zahvala

Veliku zahvalu upućujem mentoru dr.sc. Damiru Deliji, na pomoći i suradnji tijekom izrade diplomskog rada.

Zahvaljujem se svim kolegicama i kolegama na suradnji i druženju tijekom cijelog studiranja.

Zahvalnost iskazujem svojoj obitelji, a posebno sinovima Karlu i Luki, na podršci i na vremenu koje sam proveo studirajući, umjesto s njima.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme diplomskog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Forenzika mobilnih uređaja vrlo je važna grana digitalne forenzike. Prateći suvremene trendove u svijetu, razvoj mobilnih uređaja nameće se kao trend i predstavlja jednu od najbrže rastućih industrija. Sve širi razvoj brojnih funkcionalnosti i mogućnosti koje su dostupne na pametnim mobilnim uređajima dovodi po jačanja potrebe uređaja kako za poslovne, tako i za privatne svrhe. Sve veća količina podatka nalazi se u mobilnim uređajima i ukoliko dođe do bilo kojeg oblika oštećenja uređaja, gubitka podataka i/ili uređaj bio uključen u zlonamjerne radnje, forenzika mobilnih uređaja pruža niz alata kojima je moguće napraviti povrat gotovo svih podataka o korištenju mobilnog telefona. Upravo navedene činjenice daju na važnosti digitalnoj forenzici mobilnih uređaja, kao i forenzičarima i ispitivačima koji se njome bave.

Budući da mobilni uređaji sadrže vrlo vrijedan materijal u kriminalističkim istragama, forenzičari se služe svim sredstvima i metodama kako bi došli do podataka. Podaci koji su izbrisani od strane korisnika, tehnički nisu izbrisani iz memorije. Ono što digitalnim forenzičarima predstavlja problem je mobilna enkripcija kojom se služi sve veći broj tvrtki u IT sektoru, koje svjesne rizika po svoje informacije uslijed gubitka ili otuđenja mobilnih uređaja posežu za enkripcijom i udaljenim upravljanjem mobilnih uređaja.

Korištenjem alata koji su prikazani u ovom radu, prikazano je da je moguće doći do raznih vrsta podataka i dokumenata koje su korisnici ranije pobrisali s uređaja. Digitalna forenzika nije isključivo vezana uz kibernetički kriminal. Ona je vezana uz bilo kakvu istragu organiziranog kriminala pomažući na način da se otkrije komunikacija među korisnicima. Pitanja na koja digitalni forenzičar mora odgovoriti tijekom istrage su: Tko, što, gdje i kako?

Razvoj mogućnosti, pad cijena i dostupnost mobilnih uređaja, te njihovo svakodnevno korištenje povećava i porast računalnih zločina te povećava potrebu za što boljom sigurnosti. Forenzički vještaci, na temelju postojećih znanja i forenzičkih alata, moraju neprekidno proširivati svoja znanja i vještine kako bi uvijek bili jedan korak ispred počinitelja.

Ključne riječi: mobilni uređaj, korisnici, sadržaj, forenzika, analiza

Abstract

Mobile device forensics is a very important branch of digital forensics. Following the current trends in the world, the development of mobile devices is emerging as a trend and is one of the fastest growing industries. The ever-expanding development of the many functionalities and capabilities available on smart mobile devices is driving the need for devices for both business and private purposes. An increasing amount of data is in mobile devices and if any form of device damage, data loss and / or device involvement is involved in malicious activity, mobile forensics provides a variety of tools that can recover almost all data on cell phone usage. These facts give importance to digital forensics of mobile devices, as well as to forensic scientists and examiners dealing with it.

Because mobile devices contain very valuable material in criminal investigations, forensics use all means and methods to obtain information. Data that has been deleted by the user is not technically deleted from memory. What makes digital forensics a problem is mobile encryption, which serves a growing number of companies in the IT sector, who, aware of the risks of their information due to the loss or alienation of mobile devices, are reaching for encryption and remote management of mobile devices.

Using the tools presented in this paper, it is shown that it is possible to access various types of data and documents previously deleted by users from the device. Digital forensics is not solely related to cybercrime. It is linked to any organized crime investigation, helping to detect communication between users. The questions a digital forensic scientist must answer during an investigation are: Who, what, where and how?

The development of capabilities, the decline in prices and the availability of mobile devices and their daily use increases the rise of computer crimes and increases the need for the best possible security. Forensic experts, based on existing knowledge and forensic tools, must continually expand their knowledge and skills so that they are always one step ahead of the perpetrator.

Keywords: mobile, users, content, forensics, analysis

Sadržaj

1. Uvod 1

2. Forenzika 2

2.1. Općenito o forenzici 2

2.2. Mobilna forenzika 4

2.3. Priprema okruženja 4

2.3.1. Pristup mobilnoj forenzici 6

2.3.2. Priprema istrage 7

2.3.3. Izuzimanje i izolacija 7

2.3.4. Faza akvizicije 8

2.3.5. Ispitivanje i analiza 9

3. Android arhitektura 10

3.1. Struktura Android operativnog sustava 10

3.1.1. Linux jezgra 12

3.1.2. Razina apstrakcije hardvera 12

3.1.3. Android Runtime 12

3.1.4. Izvorne C / C++ biblioteke 12

3.1.5. Java API okvir 13

3.1.6. Aplikacijski sloj 13

3.2. Struktura datotečnog sustava Android 14

3.3. Pregled direktorija 16

3.3.1. Pohrana aplikativnih podataka na Android uređaje 17

3.4. Pregled tipova datotečnih sustava Android uređaja 20

3.4.1. Uobičajeni Android datotečni sustavi 21

3.4.2. Datotečni sustavi flash memorija 21
3.4.3. Datotečni sustavi bazirani na medijima 22
3.4.4. Pseudo datotečni sustavi 23
4. Metode ekstrakcije podataka 25
4.1. Android Debug Bridge (ADB) 25
4.2. Logička ekstrakcija podataka 27
4.2.1. Ručna ADB ekstrakcija 29
4.2.2. ADB Dumpsys 31
4.3. Fizička ekstrakcija podataka 33
4.3.1. Fizička ekstrakcija podataka dd alatima 34
4.3.2. Fizička ekstrakcija podataka nand alatom 36
4.3.3. Fizička ekstrakcija podataka ACQUIRE alatom 36
4.3.4. JTAG ekstrakcija 39
4.3.5. Odlemljivanje čipova 42
5. Povrat obrisanih podataka 44
5.1. Oporavak podataka sa SD kartica 45
5.2. Oporavak izbrisanih zapisa iz SQLitea baze podataka 46
5.3. Oporavak podataka iz interne memorije 47
6. Alati za forenzičku analizu Android platforme 49
6.1. EnCase Mobile Investigator 49
6.2. UFED Ultimate 51
6.3. Autopsy 53
7. Analiza preuzetih slika uređaja 55
7.1. Slika uređaja 55
7.2. Analiza slike uređaja alatom Autopsy 56
Zaključak 66

Popis kratica 67

Popis slika 69

Literatura 71

Prilog 1 – Primjer izvještaja sadržaja interne memorije mobilnog uređaja Samsung Galaxy S4 – SGH-M919 73

1. Uvod

Mobilni uređaji, pametni telefoni, su suvremeni, višenamjenski telekomunikacijski uređaji koji su postali dio svakodnevnice. Lako su dostupni krajnjim korisnicima, a nude mnoge funkcionalnosti. Moderni mobilni telefoni pohranjuju velike količine korisničkih telekomunikacijskih podataka, tako da im je inicijalna osnovna namjena, ostvarivanje glasovnih poziva pala u drugi plan. Danas se koriste za pristup internetskim sadržajima, te posjeduju razne multimedijske funkcionalnosti poput digitalne kamere, snimača zvuka, navigacije, i slično.

Sve navedeno čini mobilni uređaj bogatim izvorom bilo privatnih, bilo poslovnih podataka. Jedna od grana digitalne forenzike, forenzika mobilnih uređaja, postala je nezaobilazna u različitim postupcima i istragama, od privatnih, korporativnih do kriminalističkih. Potreba za pronalaženjem, oporavkom i analizom podataka u elektroničkom obliku sve je veća, bilo da se radi o istraživanju zlonamjernih postupaka ili proaktivnim istragama koje za cilj imaju povećanje korporativne sigurnosti podataka.

U ovom radu će biti prezentirane mogućnosti mobilnih uređaja kao izvora podataka koje forenzičarima omogućavaju dolazak do ključnih i neoborivih dokaza u istragama, kao i alati koji se koriste. Uz to biti će pojašnjeni načini dohvata podataka iz mobilnih uređaja, a na kraju i analiza sadržaja memorijske slike mobilnog uređaja.

2. Forenzika

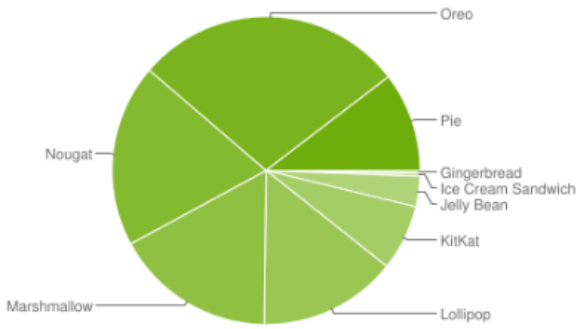
2.1. Općenito o forenzici

Budući da nije jednostavno pronaći definiciju digitalne forenzike, najčešće se u literaturi izvodi iz one autora Ken-a Zatyko. On je obnašao je funkciju direktora Defense Computer Laboratory-a gdje je vodio najveći međunarodno priznati i akreditirani laboratorij za računalnu forenziku. U vrijeme obnašanja funkcije u tom laboratoriju radilo je preko devedeset zaposlenika koji su zatvorili više od 900 slučajeva, te analizirali više od 120 terabajta podataka čiji su rezultati prezentirani na više od 70 vojnih i saveznih suđenja. Prema njemu definicija pojma digitalne forenzike svodi se na slijedeće: "Primjena računalne znanosti i istražnih postupaka u pravnu svrhu koja uključuje analizu digitalnih dokaza nakon odgovarajućeg ovlaštenja za pretraživanje, osiguranje lanca čuvanja, matematičku validaciju, korištenje validiranih alata, ponovljivost, izvještavanje i moguće stručno predstavljanje."[1]

Posebno područje digitalne forenzike koje će biti obrađeno u ovom radu je forenzika mobilnih uređaja. To je područje digitalne forenzike koje se mora brzo razvijati, budući da prati stalni napredak i razvoj mobilnih uređaja. Danas najviše zastupljene platforme mobilnih uređaja su Apple iOS koji se trenutno koristi u verziji 12, s time da je na stranicama proizvođača dostupna i verzija 13 za pregled, a svakako najzastupljeniji operativni sustav mobilnih uređaja je Android kojim ćemo se u ovom radu i baviti. Android se u najvećem postotku koristi u verzijama 6.0, zatim 8.1 i verziji 8.0, kako pokazuje Slika 2.1 Relativan broj uređaja po verzijama Android platforme.

[1] https://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics (30.3.2019.)

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.2%
4.2.x		17	1.5%
4.3		18	0.5%
4.4	KitKat	19	6.9%
5.0	Lollipop	21	3.0%
5.1		22	11.5%
6.0	Marshmallow	23	16.9%
7.0	Nougat	24	11.4%
7.1		25	7.8%
8.0	Oreo	26	12.9%
8.1		27	15.4%
9	Pie	28	10.4%



Data collected during a 7-day period ending on May 7, 2019
Any versions with less than 0.1% distribution are not shown.

Slika 2.1 Relativan broj uređaja po verzijama Android platforme[2]

Tehnološki napredak danas je rastući kao nikad prije, a taj rast je posebno izražen na području mobilnih uređaja. Namjena im danas nije samo za ostvarenje govorne i komunikacije tekstualnim porukama, nego mnogo šire, kao na primjer komunikacija putem elektroničke pošte, raznim aplikacijama za razmjenu instant poruka (Viber, WhattsApp, Telegram, itd), pregledavanje internetskih sadržaja, fotografiranje i snimanje video zapisa, satelitsku navigaciju upotrebom GPS (engl. *Global Positioning System*) sustava i raznim drugim poslovno specifičnim primjenama. Činjenica je da su u mobilnim uređajima

[2] https://developer.android.com/about/dashboards (05.07.2019.)

pohranjeni mnogi osjetljivi osobni i poslovni podaci koji gubitkom ili otuđenjem mobilnog uređaja mogu doći u posjed neželjenih osoba, a vrijednost podataka je najčešće veća od vrijednosti uređaja. Zbog toga su često ciljevi napada članovi uprave tvrtki ili voditelji financija unutar njih.

To posebno dolazi do izražaja u posljednje vrijeme, kod primjerice, terorističkih napada, kada se napadi dogovaraju i organiziraju putem mobilnih uređaja, bilo putem spomenutih servisa za razmjenu poruka ili putem socijalnih mreža. U takvom slučaju mobilni uređaji su jedino sredstvo putem kojem službe mogu doći do podataka o organizatorima, suučesnicima, a i daljnjim planovima terorista ili drugih napadača.

2.2. Mobilna forenzika

Forenzika mobilnih uređaja je dio forenzike koji se bavi izdvajanjem, oporavkom i analizom digitalnih dokaza iz mobilnih uređaja koji uključuju sve podatke u mobilnim uređajima, kao npr. SMS poruke, kontakte, poruke elektroničke pošte, dokumente , fotografije, video zapise itd. Također mobilna forenzika uključuje obnavljanje podataka izbrisanih sa uređaja korištenje različitih forenzičkih tehnika. Za cijeli taj postupak važno je da osigura integritet podataka kako bi dobiveni rezultati bili vjerodostojan dokaz. Zbog toga se sve analize rade na preslici memorije uređaja, a ne na uređaju koji je predmet forenzičke analize. Termin forenzički koristi se u digitalnoj forenzičkoj zajednici kao sinonim za pravilno rukovanje digitalnim tragovima. Mobilna forenzika, a poglavito android forenzika strelovito se razvija pogonjena razvojem mobilnih uređaja baziranih android platformom. Svaki forenzički postupak, uz to što mora osigurati nepromjenjivost dokaza, mora sadržavati i dokumentiranje svakog koraka forenzičke analize. Dokumentiranje mora obuhvaćati sve korake analize od samog početka, budući da je istraga ispravna samo u slučaju kada čuva izvorne forenzičke podatke te potvrđuje njihov integritet i valjanost. Potvrđivanje integriteta razumijeva usporedbu digitalnog otiska prije početka prikupljanja digitalnih dokaza i po završenom postupku. Sam postupak mobilne forenzike i njezini postupci ovise o platformi na kojoj se provode, pa tako poznajemo danas najčešće Android i iOS forenziku.

2.3. Priprema okruženja

Forenzičari tijekom rada mogu naići na veliki broj različitih proizvođača i modela mobilnih uređaja koji su predmet istraga. Dakle, potrebno je uspostaviti osnovno okruženje, povrh

kojeg se može raditi analiza uređaja različitih proizvođača, budući da svaki ima svoje specifičnosti. Također je vrlo važno da forenzičar održava potpunu kontrolu nad okolinom u svakom trenutku, kako ne bi došlo do neočekivanih situacija. Postavljanje odgovarajućeg laboratorijskog okruženja važan je dio forenzičkog procesa.

Android forenzička postava obično uključuje sljedeće korake:

- Upotreba novo instaliranog i forenzički čistog računalnog okruženja, što znači da nema nikakvih zaostalih ni nepotrebnih podataka u sustavu ili ako su neophodni, da su pohranjeni na način koji sprečava da ostavljanje tragova na aktualnu istragu.
- Instaliranje osnovnih upravljačkih programa potrebnog za povezivanje s uređajem. Alati za Android forenziku i metodologije raditi će na Windows, Linux i OS X platformama.
- Forenzičar mora dobiti pristup uređaju, ili mora sam biti u mogućnosti omogućiti nesmetan dohvat podataka sa mobilnog uređaja.
- Mora imati instaliran *Android Software Development Kit* (SDK) koji u razvojnom okruženju omogućuje uklanjanje pogrešaka aplikacija za pokretanje na Androidu. Uz to su potrebne aplikacije za forenzičku analizu, početna dokumentacija koja služi kao uvod u slučaj i druge alate koji bi mogli biti od pomoći tijekom istrage

Jako koristan alat u forenzičkoj analizi je emulator. Emulator je aplikacija koja omogućuje istražitelju da razumije kako se ponašaju određene aplikacije i kako se izvršava instalacija aplikacije, te kakav to ima utjecaj na uređaj i druge aplikacije. Prednost emulatora je što se može instalirati u željenoj verziji. Ovo je posebno korisno za rad s uređajima koji rade na starijim verzijama Androida.

Ono što je važan preduvjet je i mobilni uređaj sa korijenskim (engl. *root*) pravima pristupa. Omogućavanje *root* pristupa je proces kojim se korisnicima Android telefona omogućuje da dobiju najveću privilegiju, tj. privilegiju *root* korisnika na Android telefonu, što implicira prava pristupa na mape i datoteke nedostupne standardnom korisniku mobilnog uređaja. Android se temelji na Linuxu kako je i spomenuto, dakle, dobivanje *root* pristupa isto je kao i *root* pristup korisničkom ili administrativnom pristupu na Linux OS.

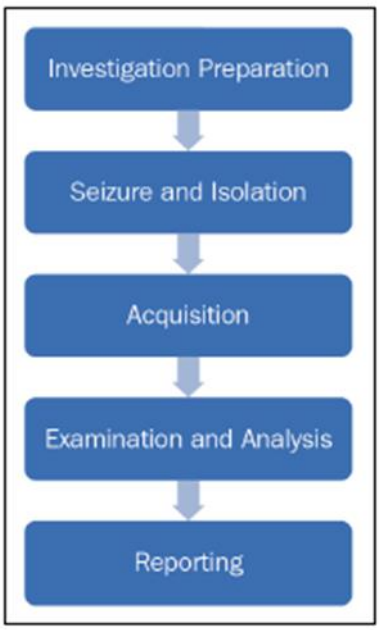
Omogućavanjem *root* prava na Android uređaju moguće je mijenjati ili zamijeniti sistemske aplikacije i postavke, pokretati specijalizirane aplikacije za koje su potrebna dopuštenja administratora uređaja ili obavljati operacije koje su inače nedostupne standardnom Android korisniku.

Međutim, s forenzičkog stajališta, glavni razlog omogućavanja *root* pristupa je pristup dijelovima memorije mobilnog uređaja koji obično nisu dostupni. Većina javnih alata za omogućavanje *root* pristupa daje prava i nakon ponovnog pokretanja uređaja i takav alat i možemo koristiti za forenzičku analizu, ali je potrebno dati prednost onima koji ne omogućavaju stalni *root* pristup kako bi se spriječilo možebitno mijenjanje podataka.

Svakoj Android aplikaciji dodijeljen jedinstveni identifikator (engl. Unique identifier UID) i pokreće se kao zasebna, s tim da je svaka aplikacija izolirana tako da ne pristupa podacima druge aplikacije. UID dodijeljen aplikaciji pohranjuje se u (engl. Extensible Markup Language) XML datoteke u mapu /data/system. Ova datoteka, osim što pohranjuje UID-ove, pohranjuje i Android dozvole svakog programa. Privatni podaci svake aplikacije pohranjuju se na lokaciji /data/data i dostupni su samo toj aplikaciji. Stoga, tijekom istrage, podacima na ovom mjestu ne može se pristupiti ako na mobilnom uređaju nije omogućen *root* pristup - standardni korisnik ne može pristupiti podacima aplikacije.

2.3.1. Pristup mobilnoj forenzici

Kad se podaci izvuku iz uređaja, koriste se različite metode analize ovisno o tome kakav je sam slučaj, tj na kojoj se grani ekspertize temelji; da li je to akademska ili istražiteljska analiza. Budući da je svaka istraga različita, nije moguće jednoznačno definirati konačni postupak za sve slučajeve, ali cjelokupni proces može se podijeliti u pet faza kako to pokazuje Slika 2.2 Proces forenzike mobilnih uređaja



Slika 2.2 Proces forenzike mobilnih uređaja[3]

2.3.2. Priprema istrage

Faza pripreme istrage počinje nakon zaprimanja zahtjeva i uključuje pripremu dokumenata i obrazaca potrebnih za dokumentiranje lanca kontrole dokaza (engl. *Chain of custody*). Tu još spadaju i podaci o vlasništvu, modelu uređaja, svrsi, informacijama koje tražitelj traži i tako dalje. Lanac kontrole dokaza odnosi se na kronološku dokumentaciju ili papirnati trag koji pokazuje izuzimanje, čuvanje, kontrolu, prijenos, analizu i raspolaganje fizičkim ili elektroničkim dokazima. Iz podataka zaprimljenih od podnositelja zahtjeva, važno je jasno razumjeti detalje cilja za svako ispitivanje.

2.3.3. Izuzimanje i izolacija

Rukovanje uređajem tijekom izuzimanja svodi se na prenošenje uređaja pomoću Faraday vrećica dizajniranih za zaštitu elektroničkih komponenti od oštećenja nastalih statičkim elektricitetom. Najvažnija misao koju moramo imati na umu je da naši postupci nemaju nikakav utjecaj na podatke pohranjene u uređaju, odnosno da ih ne modificiraju. Uz to važno je da forenzičar ne propusti bilo koju činjenicu koja može pomoći istrazi.

[3] Oleg Skulkin, Donnie Tindall, Rohit Tamma; Learning Android Forensics Second Edition; Packt; December 2018

Imajući na umu navedene činjenice i budući da danas većina uređaja ima uključeno zaključavanje zaslona, ukoliko je moguće tijekom izuzimanja potrebno je isključiti zaključavanje zaslona uz pomoć korisnika. Ako je pak uređaj otključan treba pokušati promijeniti postavke uređaja da bi omogućili veća prava pristupa uređaju. Jedna od postavki koje to omogućuju je ADB (engl. *Android Debug Bridge*). Obično se nalazi u postavkama mobilnog uređaja, a od Android verzije 4.2 je skrivena iza postavke „O telefonu“ na način da se izbornik „Broj verzije“ mora dodirnuti sedam puta. Uz to potrebno je uključiti opciju „Zaslon uključen“ i priključiti uređaj na punjač kako se uređaj ne bi zaključavao. Ova opcija također se nalazi u „Opcijama razvoja“. Ove postavke mogu se nalaziti i na drugim mjestima u meniju uređaja u ovisnosti o proizvođaču uređaja.

U postupcima mobilne forenzike od presudne je važnosti zaštititi uređaj tako da interakcija forenzičara s dokazima ne mijenja dokaze. Tu također spadaju i utjecaji napadača ili programskih rješenja za udaljeno upravljanje mobilnih uređaja – nužno je spriječiti da izuzeti uređaj ima pristup mobilnoj mreži. Velika je vjerojatnost da će napadač pokušati udaljeno brisanje svih podataka u uređaju, uključujući elektroničku poštu, aplikacije, fotografije, kontakte i druge datoteke na uređaju. To se može učiniti prijavom na Google račun koji je konfiguriran na mobilnom uređaju. Pomoću ovog softvera napadač također može locirati uređaj što može predstavljati sigurnosni rizik. Da bi uređaj izolirali iz mreže, moramo ga staviti u način rada u zrakoplovu. Način rada u zrakoplovu onemogućuje funkcije bežičnog prijenosa svih vrsta sa mobilnog uređaja, bilo putem mobilnih mreža ili putem *WLAN-a* (engl. *Wireless local area network*) i *Bluetooth*-a. No, kako je u današnje vrijeme *WLAN* dostupan i u zrakoplovima, neki uređaji sada omogućuju takav pristup u zrakoplovnom načinu pa to moramo imati na umu. Zbog svega navedenog izoliranje uređaja od svih izvora komunikacije izuzetno je važno.

2.3.4. Faza akvizicije

Faza akvizicije odnosi se na vađenje podataka iz uređaja. Sigurnosne značajke mobilnih uređaja onemogućavaju jednostavno dohvaćanje podataka, a metoda ekstrakcije ovisi o verziji operativnog sustava, proizvođaču i modelu uređaja. Uglavnom, generalizirano razlikujemo slijedeće metode akvizicije podataka:

- Ručna akvizicija je najjednostavnija od svih metoda ekstrakcije. Istražitelj koristi korisničko sučelje telefona za pregled i istragu. U ovoj metodi nisu potrebni nikakvi posebni alati i tehnike, ali ograničenje je što se mogu izdvojiti samo podaci dostupni

kroz korisničko sučelje. Ova metoda može se koristiti za provjeru podataka ekstrahiranih drugim metodama akvizicije. Važno je za spomenuti da ova metoda mijenja same podatke na uređaju, pa treba provoditi temeljito dokumentiranje postupka.

- Logička akvizicija, drugim imenom, logička ekstrakcija. Odnosi se na ekstrakciju datoteka koja se naziva i logičko vađenje, uglavnom se odnosi na vađenje podataka koji se nalaze pohranjeni u logičkoj strukturi kao što je particija datotečnog sustava. Ova vrsta ekstrakcije uključuje dobivanje tipova podataka poput tekstualnih poruka, povijesti poziva, popisa kontakata, GPS podatke, povijest internetskih preglednika, slika s telefona itd. Tehnika logičke ekstakcije funkcionira koristeći originalnu opremu proizvođača (engl. *Applications Programming Interfaces) APIs* za usklađivanje sadržaja telefona s računalom. Akvizicija datotečnog sustava logički je postupak i obično se odnosi na ekstrakciju cjelovitog datotečnog sustava s mobilnog uređaja. Akvizicija datotečnog sustava ponekad može pomoći i u vraćanju izbrisanih sadržaja (pohranjenih u *SQLite* datotekama) s uređaja.
- Fizička akvizicija uključuje izradu bit po bit kopiju čitave flash memorije uređaja, što je ekvivalent punoj slici tvrdog diska. Podaci izvađeni pomoću ove metode su obično u obliku neobrađenih podataka (u obliku slike cijele flash memorije). Ti podaci se dalje mogu analizirati kako bi se dobili podaci o datotečnom sustavu ili podaci razumljivi ljudima. Sve daljnje analize i istrage rade se na slici sadržaja memorije uređaja tako da originalni dokazi ostaju nepromijenjeni.

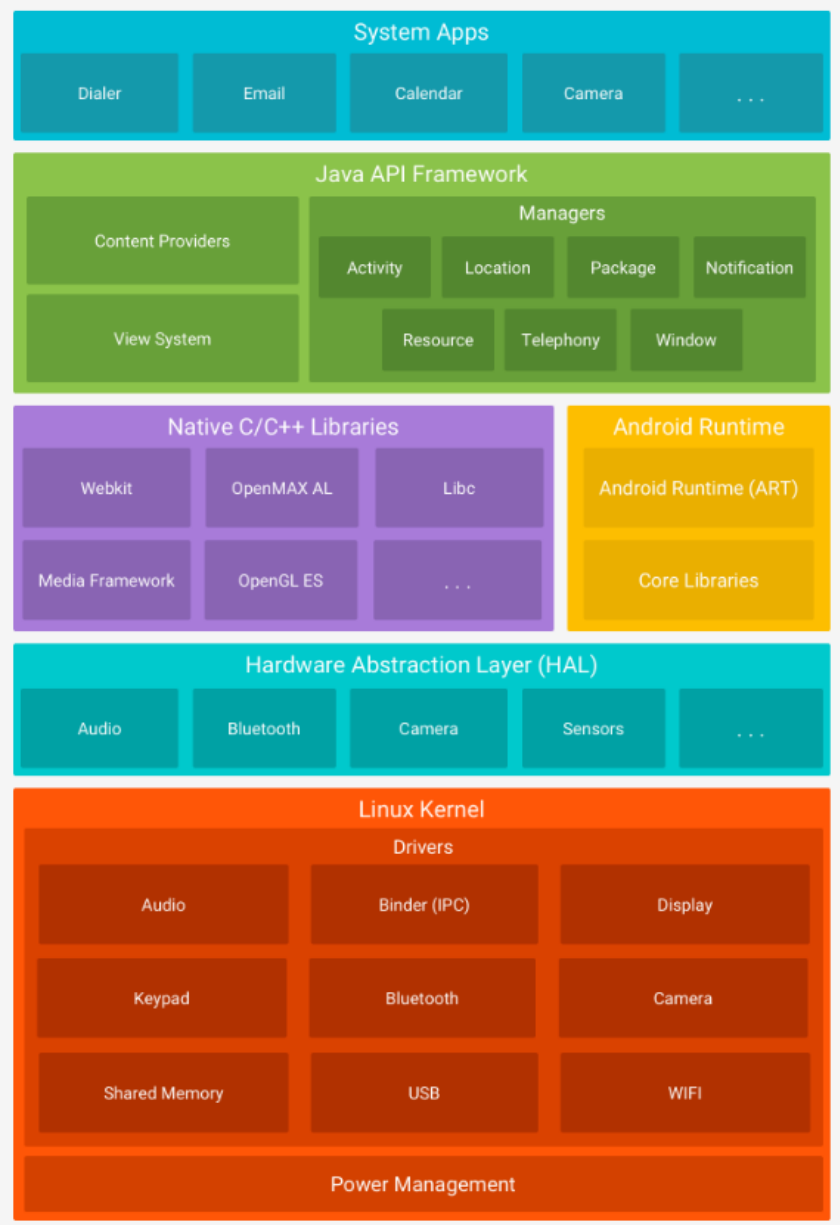
2.3.5. Ispitivanje i analiza

U ovoj se fazi ekstrakcije koriste različiti programski alati za izvlačenje podataka iz preslike memorije uređaja. Uz njih koriste se i heksadecimalni editori koji olakšavaju taj proces budući da ne postoji jedan alat koji se može koristiti u svim slučajevima. Uz alate jako je bitno znanje i kompetencije istraživača, poglavito o različitim datotečnim sustavima, datotekama i njihovim zaglavljima itd.

3. Android arhitektura

3.1. Struktura Android operativnog sustava

Kao i kod svakog računala, tako i kod mobilnih uređaja, operativni sustav preuzima ulogu za upravljanje resursima sustava i omogućava da aplikacije komuniciraju s hardverom radi izvršavanja određenih zadataka. Tako je i kod operativnog sustava Android. Android pokreće mobilne telefone, upravlja memorijom i procesima, osigurava sigurnost, brine o mrežnoj povezivosti itd. Android je operativni sustav otvorenog koda i većina koda je izdana pod licencom Apache 2.0. To pojednostavljeno znači da mu proizvođači mobilnih telefona mogu pristupiti, slobodno ga mijenjati i koristiti softver u skladu sa zahtjevima bilo kojeg uređaja. To je jedan od glavnih razloga njegovog širenja i popularnosti. Android operativni sustav sastoji se od stoga slojeva koji se izvode jedan iznad drugog. Svaki nivo stoga i elementi unutar svakog nivoa integrirani su na način da omoguće optimalno okruženje za rad mobilnih uređaja. Struktura samog Android operativnog sustava počiva na Linux jezgri, kako prikazuje Slika 3.1 Arhitektura android platforme.



Slika 3.1 Arhitektura android platforme[4]

[4] https://developer.android.com/guide/platform (14.07.2019.)

3.1.1. Linux jezgra

Android operacijski sustav baziran je na Linux jezgri (engl. *kernel*) sa određenim promjenama arhitekture koje je napravio Google kao autor izmjena. Linux je odabran jer se lako prilagođava različitim vrstama hardvera, što je neophodno da bi mogao funkcionirati na puno različitih vrsta uređaja. Linux *kernel* smješten je na dnu Android platforme i omogućava razinu apstrakcije između hardvera uređaja i gornjih slojeva operacijskog sustava. Kao što je prikazano na slici, jezgra sadrži upravljačke programe koji omogućuju komunikaciju sa *WLAN*-om, *Bluetooth*-om, *USB*-om, zvučnim podsustavom, zaslonom itd. Uz to Android ima i druge funkcionalnosti kao što su upravljanje procesima, memorijom, upravljanje sigurnosnim postavkama i umrežavanjem kojima također upravlja Linux jezgra.

3.1.2. Razina apstrakcije hardvera

Razina apstrakcije hardvera (engl. *Hardware abstraction layer*) *HAL* omogućava višoj razini, Java API okviru, rad s hardverom mobilnog uređaja uz pomoć standardnih sučelja. Ta funkcionalnost je moguća zahvaljujući višestrukim bibliotečnim modulima (engl. *libraries*), koji pružaju sučelja za različite vrste hardverskih komponente, kao što su *Bluetooth* ili kamera.

3.1.3. Android Runtime

Od verzije Androida 5.0 svaka aplikacija pokreće se u vlastitom procesu i sa vlastitom instancom *Android Runtime-a* (ART) i omogućuje pokretanje više virtualnih računala sa malim memorijskim zahtjevima izvršavanjem *Dalvik Executable* (DEX) datoteka. Spomenimo da je prije verzije Androida 5.0 *Dalvik* bio Android *Runtime*, tako da aplikacije razvijene za Dalvik trebaju raditi pri pokretanju s *ART*-om.

3.1.4. Izvorne C / C++ biblioteke

Mnoge osnovne komponente i servisi Android sustava, uključujući one ranije spomenute, poput *HAL*-a i *ART*-a, programirane su u izvornom kodu, pa im je potrebna izvorna biblioteka napisana u programskim jezicima C i C++.

3.1.5. Java API okvir

Java API okvir omogućava programerima da stvaraju aplikacije upotrebom modularnog sustava komponenti i servisa kao sastavnih dijelova za:

- Sučelje - omogućuje izgradnju korisničkog sučelja aplikacije i uključuje izbornike, rešetke, tekstualne okvire, gumbe i slično.
- Upravitelj resursa omogućuje pristup komponentama nekodirane aplikacije, poput lokaliziranih nizova, grafičkih datoteka i datoteka izgleda.
- Upravitelj obavijesti aplikacijama omogućuje prikazivanje prilagođenih upozorenja.
- Upravitelj aktivnosti upravlja životnim ciklusom aplikacija, a i njihovih pozadinskih procesa, tj redoslijedom otvaranja aktivnosti
- Davatelji sadržaja omogućuju aplikacijama pristup podacima drugih aplikacija i dijeljenje svojih podataka

3.1.6. Aplikacijski sloj

Najviši sloj u Androidu sastoji se od aplikacija (koje se nazivaju *apps*) i s njima korisnici izravno komuniciraju.

Postoje dvije vrste aplikacija:

- Sistemske aplikacije - Predinstalirane su u mobilni uređaj i isporučuju se s istim. Tu spadaju internetski preglednik, klijent elektroničke pošte, kontakti, aplikacija za telefonske razgovore i slično. Ove aplikacije generalno se ne mogu deinstalirati ili mijenjati od strane korisnika, nego na nekim uređajima samo onemogućiti. U tom slučaju ona i dalje postoji na sistemskoj particiji, ali je skrivena korisniku na sučelju uređaja. Ove aplikacije nalaze se na /system particiji.
- Korisničke aplikacije - instaliraju se sa Google trgovine koja je službeni repozitorij Android aplikacija. Na tom repozitoriju postoji svakim danom sve više aplikacija, a prema službenim podacima tamo je u prosincu 2017. godine bilo oko 3,5 miliona aplikacija[5].

[5] https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/ (10.7.2019.)

3.2. Struktura datotečnog sustava Android

Da bi mogli što bolje izvršiti ciljeve forenzičke analize, a to je dobivanje željenih podataka iz uređaja, moramo znati kakvi se podaci pohranjuju na uređaj, gdje se pohranjuju, kako se pohranjuju i pojedinosti o datotečnim sustavima na kojima su podaci pohranjeni. Razlog leži u tome da bi forenzičar mogao znati gdje podatke tražiti i koju tehniku odabrati. Zato ćemo se najprije upoznati sa izgledom Android particija. Particije su način logičke organizacije podataka unutar memorije uređaja i omogućavaju logičku raspodjelu prostora za pohranu na dijelove kojima se može pristupati neovisno jedan o drugome. Izgled particije varira između dobavljača i verzija, ali postoji nekoliko particija na svim Android uređajima i one su najčešće Android particije koje se nalaze u većini uređaja:

- BOOT: Kao što ime sugerira, ova particija sadrži potrebne podatke i datoteke za podizanje operativnog sustava mobilnog uređaja. Sadrži jezgru i *RAM* (engl. *Random-access memory*), te bez ove particije mobilni uređaj ne može pokrenuti procese.
- CACHE: Ova se particija koristi za pohranu podataka kojima se često pristupa i razne druge datoteke poput logova za oporavak i paketa za ažuriranje koji se preuzimaju putem mobilnih mreža.
- OPORAVAK (engl. *recovery*): Particija za oporavak omogućuje podizanje operativnog sustava mobilnog uređaja u konzoli za oporavak, a uz pomoć konzole se obavljaju aktivnosti poput ažuriranja telefona i drugih vrsta održavanja. U nužnom slučaju na toj particiji postoji minimalna slika za pokretanje sustava Android.
- SUSTAV (engl. *system*): Sve glavne komponente osim *kernela* i *RAM* disk-a su pohranjene na ovoj particiji. Slika Android sustava na ovoj particiji sadrži Android *libraries*, binarne datoteke sustava i unaprijed instalirane aplikacije. Bez ove particije, uređaj se ne može pokrenuti u uobičajeni način rada.
- USERDATA: Ova se particija obično naziva podatkovna particija i to je unutarnja pohrana podataka o aplikacijama gdje se pohranjuje najveći dio korisničkih podataka i tu će se nalaziti većina forenzičkih dokaza. Pohranjuje sve podatke aplikacija i standardne komunikacije.

Da bi se obavila forenzička analiza na bilo kojem sustavu, uz izgled Android particija, važno je poznavanje hijerarhije datoteka. Razumijevanje načina kako Android organizira svoje

podatke u datotekama i mapama pomažu forenzičkom analitičaru da suzi svoje istraživanje na određene lokacije. Taj operativni sustav pohranjuje datoteke slično Linuxu, pa ako to razumijemo shvatit ćemo hijerarhiju datoteka Androida vrlo dobro. U Linuxu je hijerarhija datoteka jedno stablo s vrhom koji se označava kao / i naziva se *root*. To se razlikuje od koncepta organiziranja datoteke u operacijskom sustavu Windows.

Hijerarhija Android datoteka je prilagođena verzija postojeće Linux hijerarhije. U ovisnosti o proizvođaču i temeljna verzija Linuxa, struktura ove hijerarhije može imati nekoliko manje značajnih promjena. Kako bi vidjeli kompletnu hijerarhiju datoteka, koja je vidljiva na Slika 3.2 Hijerarhija Andoid datoteka, potreban je *root* pristup.

```
j7xelte:/ # ls
acct                    init                          mnt                          res
bugreports              init.baseband.rc              nonplat_file_contexts        root
cache                   init.environ.rc               nonplat_hwservice_contexts   sbin
charger                 init.power.rc                 nonplat_property_contexts    sdcard
config                  init.rc                       nonplat_seapp_contexts       sepolicy
cpefs                   init.rilchip.rc               nonplat_service_contexts     storage
d                       init.samsungexynos7870.rc     oem                          sys
data                    init.samsungexynos7870.usb.rc plat_file_contexts           system
default.prop            init.target.rc                plat_hwservice_contexts      ueventd.rc
dev                     init.usb.configfs.rc          plat_property_contexts       ueventd.samsungexynos7870.rc
efs                     init.usb.rc                   plat_seapp_contexts          vendor
etc                     init.wifi.rc                  plat_service_contexts        vndservice_contexts
fstab.samsungexynos7870 init.zygote32.rc              proc
```

Slika 3.2 Hijerarhija Andoid datoteka[6]

[6] Oleg Skulkin, Donnie Tindall, Rohit Tamma; Learning Android Forensics Second Edition; Packt; December 2018

3.3. Pregled direktorija

Za bolje razumijevanje slijedi pregled direktorija operativnog sustava koji su prisutni u hijerarhiji datoteka Android mobilnih uređaja.

- Acct direktorij - Direktorij koji je točka montiranja za acct kontrolnu grupu (cgroup) koja osigurava prijavu korisnika putem korisničkih računa.
- Cache direktorij - Direktorij (/cache) u kojem Android pohranjuje podatke i komponente za aplikacije kojima se često pristupa. Brisanje cache memorije ne utječe na osobne podatke već jednostavno briše postojeće podatke koji se tamo nalaze. U ovoj se mapi nalazi i još jedan direktorij zvan Lost + found koji zadržava oporavljene datoteke (ako ih ima) kao posljedicu oštećenja datotečnog sustava, poput one koja je izazvana naglim uklanjanjem SD kartice bez naredbe *unmount* iz izbornika. Cache memorija može sadržavati forenzički relevantne artefakte, poput slika, povijesti pregledavanja i ostalih podataka o aplikacijama.
- Konfiguracijski direktorij - Ovaj direktorij sadrži konfiguracijske datoteke za SDCardFS (FAT32 emulacija kernel razine) i USB uređaje.
- Data direktorij - Sadrži privatne podatke svih aplikacija i većina korisničkih podataka pohranjuju se u ovu mapu. Ova mapa ima značajnu važnost s forenzičkog stajališta jer sadrži vrijedne podatke.
- Dev direktorij - Sadrži posebne datoteke za sve uređaje i on je *mount* točka za datotečni sustav *tempfs* koji definira uređaje dostupne aplikacijama.
- Mnt direktorij - Ovaj direktorij služi kao *mount* točka za sve datotečne sustave, unutarnju i vanjsku memoriju, SD kartice itd.
- Proc direktorij - *mount* točka za datotečni sustav *procfs* koji pruža pristup strukturi podataka kernela. Nekoliko programa koristi /proc kao izvor svojih informacija. Sadrži datoteke koje imaju korisne informacije o procesima. Na primjer, *meminfo*, prisutan u direktoriju /proc, daje informacije o memoriji.
- Sbin direktorij - Sadrži binarne datoteke za nekoliko važnih *daemon*-a (engl. *daemon*). Nije od velikog značaja iz forenzičke perspektive.
- Direktorij za pohranu - Ovdje se nalazi sadržaj SD kartice. Važno je spomenuti da SD kartica može biti ili izmjenjiva ili ugrađena u mobilni uređaj. Bilo koja aplikacija koja ima razinu prava *WRITE_EXTERNAL_STORAGE* može stvoriti datoteke ili mape na ovoj lokaciji. Tu se nalaze neke zadane mape kao što su Android, DCIM i

Preuzimanja, prisutne na većini mobitela. Slike digitalnih fotoaparata nalaze se kao zadana postavka u direktoriju (DCIM). Unutar DCIM direktorija nalaze se snimljene fotografije, videozapisi i privremena memorija minijatura (*cache* datoteke). Fotografije su pohranjene u /DCIM/Kamera. Uputa za Android razvojne inženjere objašnjava funkciju mapa za pohranu podataka koje nisu vezane za točno specifične aplikacije. Neke od tih mapa su:

1. Glazba: skener medija klasificira sve datoteke koji se nalaze ovdje kao glazbu korisnika
2. Podcasti: skener medija klasificira sve medije koji se nalaze ovdje kao podcaste
3. Melodije zvona: Ovdje prikazane medijske datoteke klasificiraju se kao melodije zvona
4. Alarmi: Ovdje prikazane medijske datoteke klasificiraju se kao alarmi
5. Obavijesti: Za zvukove obavijesti koriste se medijske datoteke na ovoj lokaciji
6. Slike: Ovdje su pohranjene sve fotografije osim onih snimljenih fotoaparatom i pohranjenih u direktoriju mapa
7. Filmovi: Svi filmovi osim onih snimljenih kamerom su pohranjeni u ovoj mapi
8. Preuzimanje: Ostala preuzimanja

- Sistemski imenik - Ovaj direktorij sadrži knjižne zapise, sistemske binarne datoteke i ostale datoteke povezane sa sustavom. Pred instalirane aplikacije koje dolaze zajedno s mobilnim uređajem također se nalaze na ovoj particiji.

3.3.1. Pohrana aplikativnih podataka na Android uređaje

Android uređaji pohranjuju puno specifičnih i osjetljivih podataka putem aplikacija koje se na njima nalaze. Načelno uz spomenute dvije glavne grupa aplikacija sistemske i korisnički instalirane aplikacije, aplikacije se detaljnije dijele na:

- Aplikacije koje dolaze s Androidom
- Aplikacije instalirane od strane proizvođača
- Aplikacije instalirane od strane pružatelja usluga mobilne telefonije
- Korisnički instalirane aplikacije

Sve ove navedene vrste aplikacija na mobilnom uređaju pohranjuju različite vrste podataka. Podaci o aplikaciji često sadrže bogatstvo informacija koje su relevantne za istragu. Najčešći korisni podaci za istragu koji se mogu naći na uređaju spadaju u grupe:

- SMS poruke
- popisi poziva
- instant poruke
- sigurnosne kopije podataka
- poruke elektroničke pošte
- kontakti
- slike
- video zapisi
- povijest pregledavanja internet sadržaja
- GPS podaci
- datoteke i dokumenti preuzeti sa interneta
- podaci instaliranih aplikacija kao što su Facebook, Instagram i slično.

Podaci pojedinih aplikacija mogu se pohraniti u internu memoriju ili na memorijsku karticu umetnutu u mobilni uređaj. U slučaju pohrane na micro SD karticu ti podaci se pohranjuju na bilo koju putanju, dok je situacija sa internom memorijom drugačija, tamo je lokacija unaprijed određena - podaci svih aplikacija instaliranih na uređaju (bilo sistemske aplikacije ili korisničke aplikacije) automatski se spremaju u poddirektorij /data imenovani po nazivu aplikacije. Na primjer, zadana Android aplikacija e-pošte ima naziv paketa com.android.email i interni su podaci pohranjeni u /data/com.android.email. Android pruža programerima određene opcije za pohranu podataka na uređaj. Opcije se mogu koristiti u ovisnosti o vrsti podataka koje treba pohraniti. Podaci koji pripadaju aplikacijama se mogu pohraniti na jednom od sljedećih mjesta:

- Zajedničke postavke - pružaju okvir za spremanje ključnih vrijednosti osnovnih tipova podataka u XML formatu. Osnovni tipovi podataka uključuju *boolean, float, int, long* i *string*. Stringovi se spremaju u UTF (engl. *Unicode Transformation Format*) i obično se spremaju na aplikacijsku putanju /data/shared_pref. Za primjer možemo uzeti aplikaciju elektronske pošte koja u navedenoj mapi sadrži tri datoteke, čiji sadržaj možemo pogledati naredbom `cat`

- Unutarnja pohrana - datoteke se pohranjuju u unutanjem prostoru za pohranu u samom uređaju, na putanji /data/<ime aplikacije>. Podaci spremljeni na ovoj putanji su privatni i ne može im se pristupiti, niti korisnik uređaja, a niti druge aplikacije, osim *root* prava pristupa. Međutim, postoje specifični slučajevi ili zahtjevi kada programer može dopustiti drugim procesima da mijenjaju i ažuriraju ove datoteke. Kako je spomenuto interni podaci svake aplikacije pohranjuju se u njezinoj mapi i od svih, najvažniji je sadržaj mape databases. On je ključan za forenzičku analizu i ti se podaci mogu vidjeti pomoću alata kao što je DB Browser za SQLite
- Vanjska pohrana - Aplikacije također mogu spremati podatke na vanjsku pohranu. Vanjska pohrana može biti uklonjivi medij poput SD kartice ili prostora za pohranu koji je ugrađen u sam mobilni uređaj i s njim se isporučuje. U slučaju prijenosne SD kartice, podaci bi se mogli upotrijebiti na drugim uređajima samo uklanjanjem SD kartice i umetanje u bilo koji drugi uređaj. SD kartice obično se formatiraju FAT32 datotečnim sustavom ali je moguće i drugim datotečnim sustavima poput EXT3 i EXT4. Za razliku od interne pohrane, vanjska pohrana nema stroge sigurnosne mjere, odnosno podaci ovdje pohranjeni su javni i mogu im pristupiti druge aplikacije pod uvjetom da imaju potrebna prava pristupa.
- SQLite baza podataka -SQLite je popularan format baze podataka prisutan u mnogim mobilnim sustavima i koristi se za strukturirano pohranjivanje podataka. SQLite je open source i, za razliku od mnogih drugih baza podataka, kompaktan je i nudi puno funkcionalnosti. Android podržava SQLite kroz namjenske API-je koje programeri mogu iskoristiti. Ove baze podataka su bogat izvor forenzičkih podataka, a datoteke baza koje koriste aplikacije obično se pohranjuju u /data/<ime aplikacije>/baza_podataka. Za forenzičke analize podaci u tim bazama su vrlo vrijedni jer često pohranjuju puno važnih podataka koje koristi pojedina aplikacija na mobilnom uređaju
- Mreža - U kontekstu aplikacija mreža se može koristiti za spremanje i preuzimanje podataka na vlastitim web baziranim servisima Za izvođenje operacija koje koriste mrežni promet mogu se koristit klase u java.net.* i android.net.* paketima. Ovi paketi pružaju programerima API-je niske razine neophodne za interakciju s mrežom, web poslužiteljima i tako dalje.

3.4. Pregled tipova datotečnih sustava Android uređaja

Za Android forenziku neophodno je razumijevanje datotečnog sustava, koji pomaže u dobivanju saznanja o načinu pohrane i ekstrakcije podataka. Ovo znanje o svojstvima i svojstvima struktura datotečnog sustava pokazalo se korisno tijekom forenzičke analize. Pojam datotečni sustav odnosi se na način na koji se podaci pohranjuju, organiziraju i formiraju datotečne cjeline. Osnovna instalacija može biti temeljena na jednom volumenu podijeljenog na nekoliko particija kojom mogu upravljati različiti datotečni sustavi. Korisnici PC računala pokretanih operativnim sustavom Microsoft Windows koriste FAT32 ili NTFS datotečne sustave, a korisnicima Linuxa poznatiji su za EXT3 ili EXT4 datotečni sustavi. Činjenica je da Linux, a tako i Android koristi točke montiranja (engl. *mount point*), a ne pogone (to jest, C: ili D :). Svaki datotečni sustav definira vlastita pravila za upravljanje datotekama na volumenu. Ovisno o tim pravilima, svaki datotečni sustav nudi različitu brzinu za preuzimanje datoteka, sigurnost, veličinu i tako dalje. S forenzičkog stajališta važno je razumjeti koje datotečne sustave Android koristi i kako identificirati datotečne sustave od značaja za istragu. Na primjer, datotečni sustav koji pohranjuje korisničke podatke za forenzičare je važniji od datotečnog sustava koji se koristi za podizanje samog operativnog sustava.

Kao što je spomenuto, Linux je poznat po tome što podržava veliki broj datotečnih sustava. Tim datotečnim sustavima koje koristi, ne pristupa imenima pogona, već se kombiniraju u jednu hijerarhijsku strukturu stabla koja predstavlja datotečni sustav kao jednu cjelinu. Svaki novi datotečni sustav dodaje se u ovo jedinstveno stablo datotečnih sustava kroz proces montiranja (engl. *mounting*). Dakle, datotečni sustavi su montirani u mape, a datoteke u tom datotečnom sustavu su sadržaj tih mapa. Ta se mapa naziva točka montiranja (engl. *mount point*). Suština takvog pristupa je da nema razlike postoji li datotečni sustav na lokalnom uređaju ili na udaljenom uređaju nego je sve integrirano u hijerarhiju jedne datoteke koja počinje korijenom. Svaki datotečni sustav ima zasebni modul *kernel*-a kojim registrira operacije kojima podržava virtualni datotečni sustav - VFS (engl. *Virtual File System*). VFS omogućuje različitim aplikacijama pristup različitim datotekama na jedinstveni način. Android *kernel* dolazi s podskupom velike zbirke datotečnih sustava u rasponu od JFS (engl. *Journal File System*) do Amiga datotečnog sustava. Svim pozadinskim radom upravlja kernel kad je instaliran datotečni sustav.

Da bi saznali koje datotečne sustave na Android uređaju podržava Android *kernel* mora se pogledati sadržaj datoteke *filesystems* u mapi /proc. Sadržaj ove datoteke može se pregledati naredbom (na uređaju Samsung galaxy J7):

```
j7xelte:/# cat /proc/fileystems
```

3.4.1. Uobičajeni Android datotečni sustavi

Datotečni sustavi korišteni u Android mobilnim uređajima mogu se podijeliti u tri glavne kategorije:

- Datotečni sustavi flash memorije
- Datotečni sustavi bazirani na medijima
- Pseudo datotečni sustavi

3.4.2. Datotečni sustavi flash memorija

Flash memorija je vrsta stalno napajane neizbrisive memorije koja se može izbrisati i reprogramirani u memorijskim jedinicama koja se nazivaju blokovi. Zbog posebnih karakteristika Flash memorije, posebni datotečni sustavi vrše pisanje i brisanje pojedinih blokova po tom mediju. Iako se podržani datotečni sustavi razlikuju ovisno o verziji Androida, uobičajeni su datotečni sustavi flash memorije sljedeći:

- *Extended File Allocation Table (exFAT)* - Microsoftov datotečni sustav optimiziran za flash diskove. Zbog zahtjeva za licencom nije dio standardnog Linux kernela. No ipak, nekoliko proizvođača pruža podršku za taj datotečni sustav.
- Flash Friendly File System (F2FS) - Samsung je predstavio kao datotečni sustav otvorenog koda. Osnovna namjera bila je izgraditi datotečni sustav koji uzima u obzir karakteristike uređaja za pohranu na temelju NAND flash memorije.
- Journal Flash File System, verzija 2 (JFFS2) - Datotečni sustav koji je strukturiran putem dnevnika u Androidu. JFFS2 je zadani flash datotečni sustav za *Android Open Source Project* (ASOP) od verzije Androida 4.0 (ICS). Datotečni sustavi poput *LogFS, UBIFS, YAFFS* koji se i dalje razvijaju zamjena su za JFFS2.
- Yet Another Flash File System version 2 (YAFFS2) - Datotečni sustav otvorenog izvornog koda, predstavljen 2002. godine. Dizajniran je za brzi rad sa NAND flash memorijama. YAFFS2 koristi OOB (engl. *out-of band*) i često nije dohvaćen ili dekodiran ispravno tijekom forenzičke analize, što značajno otežava postupak

analize. YAFFS2 je u jednom trenutku bilo najpopularnija verzija datotečnog sustava i još uvijek se jako puno koristi u Android uređajima. YAFFS2 je datotečni sustav koji je strukturiran putem loga. Integritet podataka osigurava se čak i u slučaju naglog prekida napajanja. Trenutno YAFFS2 nije podržan u novijim verzija *kernel*-a, ali neki proizvođači mobilnih uređaja i dalje ga nastavljaju podržavati.

- Robust file system (RFS) podržava NAND flash memoriju na Samsung uređajima. RFS je u suštini kao FAT16 (ili FAT32) datotečni sustav u kojem je zapisivanje omogućeno kroz transakcijski log. Mana RFS-a je kašnjenje koje za posljedicu ima usporenje cijelog Android operativnog sustava.

3.4.3. Datotečni sustavi bazirani na medijima

Osim prethodno razmotrenih datotečnih sustava flash memorije, Android uređaji obično podržavaju sljedeće medijske datotečne sustave:

- EXT2/EXT3/EXT4 - (EXTended datotečni sustav) predstavljen 1992. godine posebno za Linux kernel i bio je jedan od prvih datotečnih sustava te je koristio virtualni datotečni sustav. EXT2, EXT3 i EXT4 su sljedeće verzije. Journaling je glavna prednost EXT3 u odnosu na EXT2. Verzija EXT3 u slučaju neočekivanog isključivanja nema potrebe za provjerom datotečnog sustava. EXT4 datotečni sustav, četvrti prošireni datotečni sustav, dobio je na značaju s mobilnim uređajima koji implementiraju dvojezgrene procesore. Poznato je da je YAFFS2 datotečni sustav imaju usko grlo na dual-core sustavima. S Gingerbread verzijom Androida, YAFFS datotečni sustav zamijenjen je za EXT4.
- FAT (File Allocation Table) - datotečni sustavi poput FAT12, FAT16 i FAT32 i nativno njih podržava operativni sustav MSDOS.
- VFAT (Virtual File Allocation Table) - proširenje za FAT16 i FAT32 datotečne sustave. Microsoftov datotečni sustav FAT32 podržava većina Android uređaja. Također podržavaju ga gotovo svi glavni operativni sustavi, uključujući Windows, Linux i macOS. To omogućuje ovim sustavima da lako čitaju, mijenjaju i brišu datoteke na FAT32 particiji Android uređaja. Većina vanjskih SD kartice su formatirane pomoću datotečnog sustava FAT32.

3.4.4. Pseudo datotečni sustavi

Uz prije navedene postoje i pseudo datotečni sustavi, koji se mogu smatrati logičnim grupiranje datoteka. Neke od važnijih pseudo datotečnih sustava Android uređaja:

- cgroup pseudo datotečni sustav - omogućava način pristupa i definiranje parametara kernela, budući da ima nekoliko različitih kontrolnih skupina procesa. Popis grupa može se izlistati pozivanjem naredbe

  ```
  cat /proc/cgroups
  ```

- rootfs za Android operativni sustav najvažniji datotečni sustav koji sadrži informacije za podizanje sustava. Ovaj datotečni sustav koji „montira“ druge datotečne sustave, bez njega uređaj ne funkcionira.
- Procfs datotečni sustav sadrži informacije o strukturi kernela operativnog sustava, procesima i ostalim važnim informacijama sistema koje se nalaze u /proc mapi.
- Sysfs datotečni sustav montira /sys mapu, koja sadrži podatke o konfiguraciji uređaja. Primjer sadržaja sys mape Android uređaja:

  ```
  j7xelte:/sys # ls -1
  bcm-dhd
  block
  bus
  class
  dev
  devices
  firmware
  fs
  kernel
  mms_ts
  module
  power
  ```

  Budući da su podaci prisutni u navedenim mapama uglavnom povezani s konfiguracijom, forenzički ovi podaci nemaju neko važno značenje. Korisno može biti utoliko da se vidi da li je neka značajka uključena na mobilnom uređaju. Važno je također za spomenuti da se u ovim mapama nalazi jako puno datoteka pa da se podaci ne bi promijenili forenzičkom analizom potrebno ih je zaštititi od mijenjanja.

- tmpfs sprema datoteke u RAM (engl. *Random Access Memory*),a obično se mapira u /dev mapu. Glavna prednost korištenja RAM-a je brži pristup i preuzimanje, ali, jednom kada se uređaj isključi, ti podaci su nedostupni.

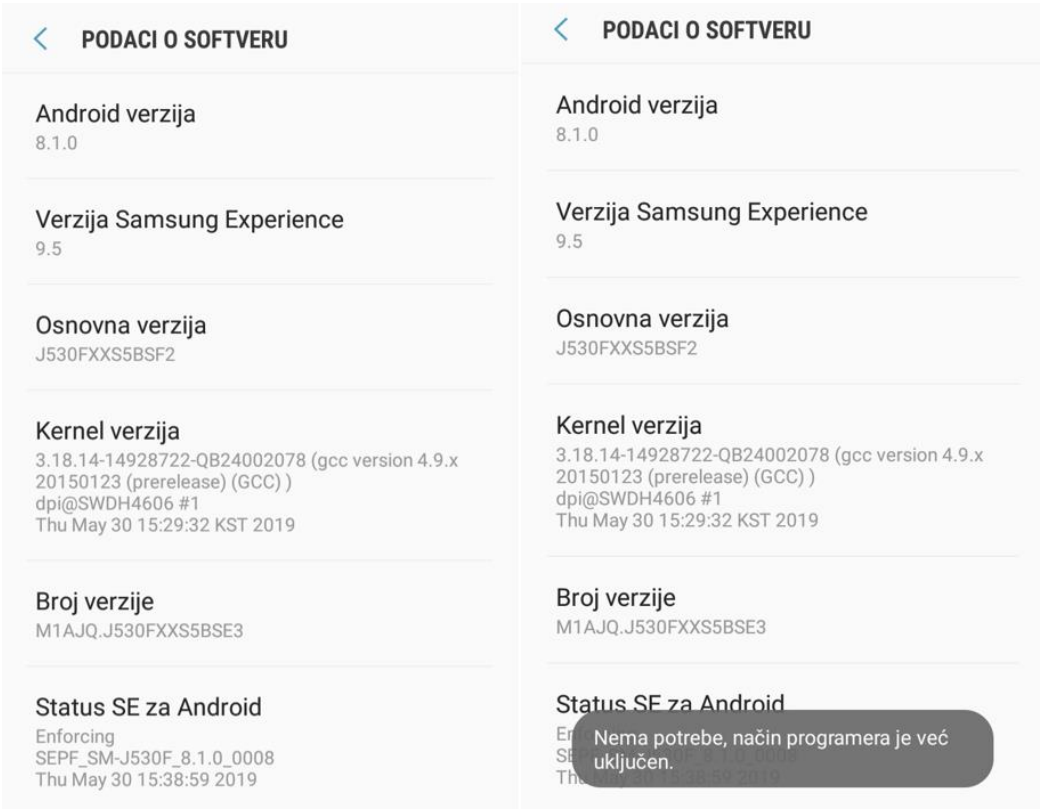
Imajući na umu sve spomenuto važno je da forenzičar ima na umu sve te spoznaju tijekom provođenja postupka izdvajanja i analize dokaza, kako ih ne bi oštetio ili narušio lanac kontrole dokaza.

4. Metode ekstrakcije podataka

4.1. Android Debug Bridge (ADB)

Za forenzičke postupke na mobilnim uređajima sa Android operativnim sustavom najvažniju ulogu ima ADB (engl. *Android Debug Bridge*).

Nalazi se na putanji `<sdk_lokacija>/platform-tools`. Da bi ADB funkcionirao mora biti uključena opcija *USB Debugging*. Ona se nalazi u postavkama/opcije za razvojne programere. Međutim, to ne mora biti tako na svim uređajima, budući da različiti uređaji imaju različita korisnička sučelja. Svaki je uređaj specifičan, što po izgledu sučelja ili dodatnim temama koje proizvođači izrađuju kako bi njihovi uređaji imali jedinstvena sučelja i time na neki način navikom korištenja zadržavali korisnike na upotrebi uređaja baš tog proizvođača. Na nekim uređajima ponekad je možda potrebno koristiti određene tehnike za pristup opcijama za razvojne programere. U takvom slučaju na uređaju treba istražiti i utvrditi način pristupa tim opcijama. Primjerice novijim generacijama Samsung uređaja opcija se aktivira nakon što sedam puta unutar izbornika podaci o softveru pritisnemo na „Broj verzije“, kako prikazuje Slika 4.1 Uključenje opcije USB Debugging (Način programera).



Slika 4.1 Uključenje opcije USB Debugging (Način programera)[7]

Jednom kada se odabere opcija USB otklanjanje pogrešaka, uređaj će pokrenuti ADB *daemon* (adbd) u pozadini i neprestano će tražiti USB vezu. *Daemon* će obično pokrenuti pod neprivilegiranim korisničkim računom i na taj način ne omogućuje pristup internim podacima o aplikaciji. Ali na mobilnim uređajima sa *root* pristupom *adbd* će se pokretati sa pravima *root* računa i pružati pristup svim podacima. Na radnoj stanici (na kojoj je instaliran Android SDK) *adbd* će se pokrenuti kao pozadinski proces. Kada se pokrene ADB klijent, prvo provjerava je li ADB *daemon* već pokrenut. Ako nije, pokreće novi postupak za pokretanje ADB *daemon*-a i oni komuniciraju putem TCP portova 5555 do 5585. Jedan port se koristi za komunikaciju sa konzolom uređaja, dok je neparni port za ADB veze. Klijentski program ADB komunicira s lokalnim *adbd*-om preko *port*-a 5037.

Nakon spajanja uređaja na radnu stanicu i prije pokretanja ADB naredbi, korisno je znati da li je Android uređaj ispravno spojen na ADB poslužitelj. To se može provjeriti pomoću naredbe *ADB devices* koja pokazuje ispis svih uređaja koji su spojeni na računalo kao na primjer:

[7] Slika zaslona mobilnog telefona autora (14.08.2019.)

```
adb devices[8]

List of devices attached

52037762b835835b device
```

Važno je imati na umu da ukoliko upravljački programi nisu instalirani, ili nisu ispravno instalirani prethodna naredba će pokazati praznu liniju jer neće biti svjesna priključenog uređaja. Ako se naiđe na tu situaciju, potrebno je preuzeti potrebne upravljačke programe sa internetske stranice proizvođača i instalirati ih. Kao što se vidi u rezultatima naredbe, odgovor te naredbe sadrži serijski broj uređaja. Serijski broj jedinstven je niz koji koristi ADB kako bi identificirao svaki Android uređaj.

Moguće vrijednosti stanja veze i njihovo značenje su sljedeće:

- *Offline*: Instanca nije povezana na ADB ili ne reagira.
- *Device*: Instanca je povezana na ADB poslužitelj.
- *No device*: Nije povezan uređaj.
- *Unauthorized*: USB otklanjanje pogrešaka nije autorizirano.

Kako je spomenuto, predstavljajući Android forenziku, Android radi na Linux kernelu i na taj način pruža pristup *shell-u*. Pomoću *ADB*-a može se pristupiti *shell-u* za pokretanje nekoliko naredbe na Android uređaju. U Linux okruženju, *shell* se odnosi na poseban program koji omogućuje interakciju s njim unošenjem određenih naredbe s tipkovnice - pri tome *shell* izvrši naredbe i prikaže svoj izlaz.

4.2. Logička ekstrakcija podataka

U digitalnoj forenzici izraz logička ekstrakcija obično se koristi za označavanje ekstrakcija koja se ne obnavlja na izbrisanim podacima ili ne uključuju potpunu kopiju dokaza. Međutim, „ispravnija definicija logičkog ekstrakcije podataka, je bilo koja metoda koja zahtijeva komunikaciju s bazom koja se nalazi unutar samog mobilnog uređaja“[9]. Zbog interakcije s operativnim sustavom, forenzičar ne može biti siguran da li je dohvatio sve podatke jer operativni sustav bira kojim podacima omogućuje vanjski pristup. U tradicionalnim računalnim forenzikama logička ekstrakcija je analogna kopiranju i

[8] https://dfir.science/2017/04/Imaging-Android-with-root-netcat-and-dd.html (30.08.2019.)
[9] Oleg Skulkin, Donnie Tindall, Rohit Tamma; Learning Android Forensics Second Edition; Packt; December 2018

lijepljenju mape radi izdvajanja podataka iz sustava i taj postupak kopira samo datoteke kojima korisnik može pristupiti i vidjeti ih. Ako je bilo skrivenih ili izbrisanih datoteka u kopiranju mape, iste neće biti u kopiranoj verziji mape.

Razgraničenje između logičke i fizičke ekstrakcije u mobilnoj forenzici nije tako jasno razgraničeno kao u tradicionalnoj računalnoj forenzici. To možemo usporediti na primjeru izbrisanih podataka koji se mogu rutinski oporavljati logičkom ekstrakcijom na mobilnim uređajima zbog samog načina sustava SQLite baze podataka koje se koriste za pohranu podataka. Nadalje, gotovo svaka mobilna ekstrakcija će zahtijevati neki oblik interakcije s operativnim sustavom Android; nema jednostavne ekstrakcije ekvivalentno izvlačenju tvrdog diska i snimanju traženih podataka bez podizanja operativnog sustava koji se nalazi na disku. Logičku ekstrakciju možemo definirati kao proces kojim dobivamo podatke vidljive korisniku, a može uključivati podatke koji su označeni za brisanje.

U tipove podataka koji se mogu logički ekstrahirati uglavnom spadaju su svi podaci o korisniku:

- kontakti
- popisi poziva
- SMS poruke / MMS poruke
- podaci o aplikacijama
- sistemski zapisi i informacije o sustavu

Većina tih podataka pohranjena je u bazama podataka SQLite, pa je čak moguće i oporaviti velike količine izbrisanih podataka logičnim izvlačenjem.

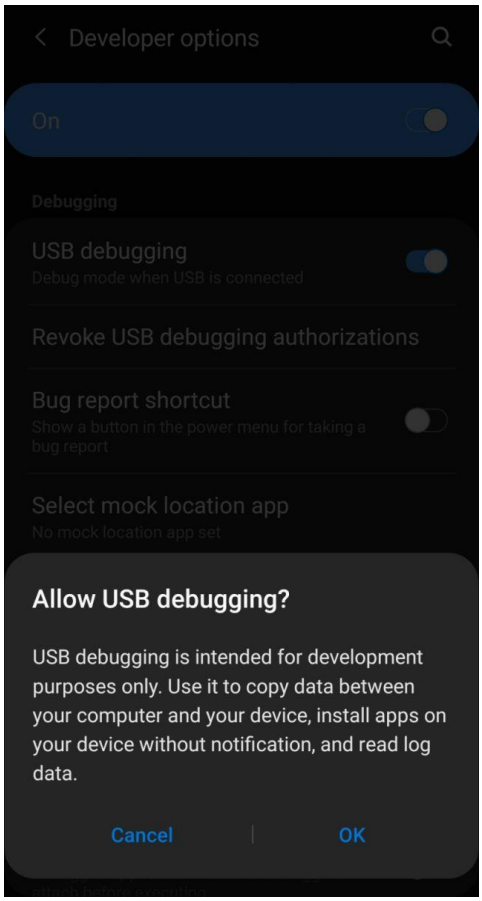
Kod logičke ekstrakcije važan je *root* pristup, jer kada se forenzički analizira Android uređaj, ograničavajući faktor često nije vrsta podataka koji se traže, nego da li forenzičar ili osoba koja istražuje uređaj ima mogućnost pristupa podacima. Svi navedeni podaci nalaze se spremljeni u unutarnjoj *flash* memoriji, zaštićenoj i za čije su čitanje potrebna *root* prava pristupa. Izuzetak su podaci o aplikacijama koji se pohranjuju na SD karticu, što ćemo spomenuti i kasnije. Bez *root* prava forenzičar ili ispitivač ne može jednostavno kopirati podatke iz */data* particija. Ispitivač će morati pronaći neku metodu eskalacije prava kako bi dobio pristup kontaktima, zapisnicima poziva, SMS/MMS i podacima aplikacije. Ove metode često nose brojne rizike, poput mogućnosti da se uređaj uništi ili se uništi mogućnost podizanja operativnog sustava (čineći uređaj neupotrebljivim).

Metode dobivanja *root* pristupa se obično razlikuju od uređaja do uređaja, a nema univerzalnog načina da se dobije takav pristup svakom uređaju. Komercijalni mobilni forenzički alati kao što su *Oxygen Forensic Detective*[10] i *Cellebrite UFED*[11] imaju ugradbene mogućnosti za privremeno i sigurno dobivanje *root* pristupa za mnoge uređaje, ali ne pokrivaju širok raspon svih Android uređaja. Odluka o dobivanju *root* pristupa na uređaju treba biti u skladu s lokalnim operativnim postupcima i mišljenjem nadležnog suda. Pravno prihvaćanje dokaza dobivenih *root* pristupom varira u ovisno o nadležnom sudskom tijelu.

4.2.1. Ručna ADB ekstrakcija

Kada imamo pripremljeno ADB okruženje kako je opisano naredba `adb pull` može se koristiti za izvlačenje pojedinih datoteka ili čitavih direktorija izravno iz uređaja na računalo forenzičara. Ova je metoda posebno korisna za male, točno definirane preglede. To možemo objasniti na primjeru istrage koja ima strogo definiran cilj analize, npr. MMS poruke. U tom slučaju forenzičar može izvršiti povlačenje samo datoteka koje sadrže MMS poruke. Da bi ekstrakcija podataka putem ADB-a funkcionirala uređaj koji se ispituje također mora biti pravilno konfiguriran. ADB je metoda putem koje će računalo forenzičara komunicirati s mobilnim uređajem. Nakon što se ADB opcija uključi kao je ranije opisano vidjet ćemo da su dostupne opcije za programere, jednostavno se uključi kako pokazuje Slika 4.2 Uključenje opcije USB otklanjanje grešaka i nakon što potvrdno odgovorimo na pitanje mobilnog uređaja, uređaj je spreman.

[10] https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective (15.09.2019)
[11] https://www.cellebrite.com/en/ufed-ultimate/ (15.09.2109.)



Slika 4.2 Uključenje opcije USB otklanjanje grešaka[12]

Slika note

Uz to a računalu je neophodno da su instalirani ispravni upravljački programi za uređaj koji želimo analizirati. Ako su na računalo instalirani komercijalni forenzički alati, izgledno su se s njima instalirani odgovarajući upravljački programi. Kada su navedeni zahtjevi ispunjeni moramo provjeriti da li na priključenom uređaju postoji *root* pristup. To se izvodi pokretanjem naredbe `adb shell`

Ovom naredbom otvoriti će se *shell* prema mobilnom uređaju i on će komunicirati sa računalom forenzičara, što znači da bilo koja naredba koje se izvodi u *shell*-u izvršavat će se na uređaju. *Shell* će se pojaviti na jedan od dva načina, bilo sa $ ili #:

U Linux sustavima # se koristi za označavanje *root* korisnika; $ označava korisnika koji nije *root*. Ako shell vraća znak #, ima korijenski pristup. Ako *shell* vrati $, pokušajte pokrenuti naredbu `su`

[12]Slika zaslona mobilnog telefona autora (14.08.2019.)

Ako je `su` naredba podržana na uređaju eskalirat će prava pristupa *shell*-a u *root* pristup. Potrebno je imati na umu da su neki stariji uređaji *shell* automatski pokrenuli kao *root*; jednostavno otvaranje *shell* ADB-a dovoljno je za *root* pristup forenzičara. Za prijenos podataka sa Android mobilnog uređaja na računalo forenzičara koristi se naredba `adb pull`

Sama sintaksa naredbe izgleda ovako:

```
adb pull –p /sdcard/Pictures/1.png D:\Test
```

gdje argument -p označava napredak prijenosa datoteka

Uz to moguće je prenositi i cijelu mapu sa slijedećom sintaksom:

```
adb pull –p /data/data D:\Test
```

To bi kopiralo svaku datoteku iz mape /data/ u mapu Test na računalu forenzičara. To nije ekvivalentno fizičkoj slici, ako su određene datoteke preskočene i izbrisane datoteke neće se kopirati, ali to je jednostavna metoda za izvlačenje velike većine podataka o aplikaciji korisnika.

4.2.2. ADB Dumpsys

Dumpsys je alat koji je ugrađen u Android operativni sustav i uglavnom se koristi u razvojne svrhe kako bi prikazao status servisa koji se pokreću na uređaju. Međutim, alat može sadržavati i forenzički zanimljive informacije. Dumpsys ne zahtijeva *root* pristup, ali kao i sve ADB naredbe, zahtijeva uključeno USB ADB na uređaju. Točni servisi koje je moguće pregledati razlikuju se ovisno o uređajima i Android verziji. Za prikaz popisa mogućih servisa koji se mogu dohvatiti mogu se identificirati slijedećom naredbom:

```
adb shell service list
```

Rezultat te naredbe je ovakav prikaz:

```
C:\platform-tools>adb shell service list
Found 136 services:
0       sip: [android.net.sip.ISipService]
1       carrier_config: [com.android.internal.telephony.ICarrierConfigLoader]
2       phone: [com.android.internal.telephony.ITelephony]
3       isms: [com.android.internal.telephony.ISms]
4       iphonesubinfo: [com.android.internal.telephony.IPhoneSubInfo]
5       simphonebook: [com.android.internal.telephony.IIccPhoneBook]
6       telecom: [com.android.internal.telecom.ITelecomService]
7       isub: [com.android.internal.telephony.ISub]
8       contexthub: [android.hardware.location.IContextHubService]
9       netd_listener: [android.net.metrics.INetdEventListener]
10      connmetrics: [android.net.IIpConnectivityMetrics]
11      bluetooth_manager: [android.bluetooth.IBluetoothManager]
12      lineagetrust: [lineageos.trust.ITrustInterface]
13      lineagestyle: [lineageos.style.IStyleInterface]
14      lineageaudio: [lineageos.media.ILineageAudioService]
15      lineagelivedisplay: [lineageos.hardware.ILiveDisplayService]
16      lineageweather: [lineageos.weather.ILineageWeatherManager]
17      lineageperformance: [lineageos.power.IPerformanceManager]
18      lineagehardware: [lineageos.hardware.ILineageHardwareService]
19      profile: [lineageos.app.IProfileManager]
20      autofill: [android.view.autofill.IAutoFillManager]
21      imms: [com.android.internal.telephony.IMms]
22      media.camera.proxy: [android.hardware.ICameraServiceProxy]
23      media_projection: [android.media.projection.IMediaProjectionManager]
24      launcherapps: [android.content.pm.ILauncherApps]
25      shortcut: [android.content.pm.IShortcutService]
```

Slika 4.3 Prikaz popisa mogućih servisa[13]

Naziv servisa smješten prije dvotočke je argument koji se koristi u kombinaciji sa naredbom `dumpsys`. To na primjeru sintakse izgleda ovako;

```
adb shell dumpsys iphonesubinfo
```

Kao odgovor ove naredbe rezultat je IMEI mobilnog uređaja.

Uz ovaj primjer postoje mnogo dumpsys servisa koji su forenzički zanimljivi, a slijedi nekoliko primjera:

- iphonesubinfo - IMEI mobilnog uređaja koji je podvrgnut forenzičkoj analizi
- batterystats - koriste se za prikazivanje upotrebe pokrenutih aplikacija
- procstats - služi za prikaz korištenja procesora pokrenutim aplikacijama, u kombinaciji s upotrebom baterije, može pokazati da je aplikacija nedavno bila aktivna

[13] Oleg Skulkin, Donnie Tindall, Rohit Tamma; Learning Android Forensics Second Edition; Packt; December 2018

- user - od verzije Androida *Jelly Bean*, Google je dodao podršku za više korisnika na tablet uređajima. Izlaskom *Lollipop*-a, Google je proširio ovu podršku na mobilne uređaje. Jedan od najizazovnijeg problema digitalne forenzike je da dokaže tko je koristio uređaj kada su izvedene inkriminirajuće radnje
- app ops - ovaj servis prikazuje kada je aplikacija posljednji put koristila svako svoje pravo pristupa
- WiFi - prikazuje popis svih SSID-ova za koje je veza spremljena, posebno je korisno ako želimo rekonstruirati kretanje mobilnog uređaja, odnosno vlasnika.

Pokretanje naredbe `dumpsys` bez naziva servisa pokreće naredbu sa svim dostupnim servisima. Budući da je rezultat takve naredbe vrlo velik i trebalo bi ga preusmjeriti u tekstualnu datoteku, na način:

```
adb shell dumpsys> dumpsys.txt
```

Time bi dobili rezultat u datoteci dumpsys.txt u trenutnoj radnoj mapi. Ta datoteka može se pretraživati ili se može pozvati skriptom za izdvajanje poznatih i relevantnih polja. *Dumpsys* je izuzetno moćan alat koji se može koristiti za prikaz informacija koje se ne mogu dobiti drugdje na uređaju. Forenzička preporuka je pokrenuti *dumpsys* na svakom Android mobilnom uređaju koji je predmet forenzičke analize, nakon što je izuzet, prije nego se ugasi, jer će se time dobiti puno korisnih informacija koje se mogu kasnije upotrijebiti u forenzičkoj analizi, budući da ne zahtijeva *root* pristup.

4.3. Fizička ekstrakcija podataka

U digitalnoj forenzici fizička ekstrakcija po definiciji je slika memorije mobilnog uređaja, dobivena bit po bit kopiranjem. U forenzici klasičnih računala taj proces uključuje izuzimanje dokaza sa računala osumnjičenika izuzimanjem diska ili drugog medija, te izrada preslike identične originalu, bez da se rade ikakve preinake na izvorniku. Slika se izrađuje pomoću blokatora pisanja bez ikakvog podizanja pogona, što rezultira datotekom slike koja sadrži točnu kopiju osumnjičenikovog diska. Produkt ovakvog postupka naziva se često RAW slike ili jednostavno binarna datoteka. Fizička ekstrakcija razlikuje se od logičke u tome što su to točne kopije memorije uređaja i uključuju neraspoređeni prostor, datotečni *slack, slack* volumena na disku itd.

U mobilnoj forenzici rezultat je isti, rezultat izrade slike mobilnog uređaja je bit po bit preslika uređaja, s napomenom da je metodologija drukčija. Primjer toga je uklanjanje *flash*

memorije iz uređaja da bi se slika mogla izraditi, što može biti dugotrajan i skup proces, a zahtijeva mnogo specijaliziranih znanja. Nadalje, ako se ne koriste napredne metode JTAG (engl. *Joint Test Action Group*) ili *chip-off*, uređaj se mora pokrenuti do određene mjere da bi se moglo pristupiti željenim podacima. Nakon toga slijedi pronalaženje alata koji može raščlaniti dobivenu konačnu sliku memorije mobilnog uređaja. Slike čvrstih diskova rađene su na sustavima koji su dugo dokumentirani i proučavani, dok se datotečni sustavi mobilnih uređaja često mijenjaju, pa time i preslike mobilnih uređaja, a uz to u nekim su slučajevima mobilni datotečni sustav čak je jedinstven za određene proizvođače mobilnih uređaja. Iz toga proizlazi da je ponekad teže doći do saznanja što učiniti sa slikom nakon što je kreirana nego izrada same preslike mobilnog uređaja koji je predmet analize.

Ako se promišlja do kojih sve podataka iz mobilnih uređaja možemo doći fizičkom ekstrakcijom, odgovor je do svih podataka. Taj detalj proizlazi iz činjenice da slika fizičke ekstrakcije točna slika uređaja i svaki podatak na uređaju nalazi se u datoteci slike. Kako je spomenuto, fizičkom ekstrakcijom forenzičar je ograničen samo njegovim mogućnostima pronalaženja relevantnih podataka. Općenito, to je zbog nedostatka dobrih alata za forenzičku analizu slika mobilnih uređaja. Situaciju analize dodatno kompliciraju pojedine aplikacije koje kodiraju korisničke podatke, tako da je analiza podataka u specijaliziranim aplikacijama ili heksadecimalnim editorima još dodatno zakomplicirana i lako se može dogoditi previd vrijednih dokaza. Zbog toga je potrebno razmotriti različite metode pregleda i analize datoteka dobivenih fizičkom ekstrakcijom. Kako je ranije spomenuto *root* pristup, kao i kod logičke ekstrakcije, izuzetno je važan i kod fizičke ekstrakcije. Da bismo izradili sliku uređaja, naredbe za to moraju se izvršiti na uređaju iz ADB ljuske (engl. *shell*), a za njihovo izvršavanje trebaju *root* prava pristupa. Ako nema *root* prava jedine preostale metode su *JTAG* ili *chip-off* metode.

4.3.1. Fizička ekstrakcija podataka dd alatima

Ekstrakcija *dd* alatom standardno se koristi na računalima tako da je poznata iz te sfere forenzike. DD je nativno Linux naredba komandne linije koja služi za pretvorbu i kopiranje datoteka. Postoje i alati za Windows platformu koji imaju istu namjenu poput *FTK imager*-a koji se također koriste za izradu bit po bit slike datotečnog sustava ili cijelih diskovnih pogona. Uz navedene često se još koriste i alati poput *dcfldd, dc3dd, ddrescue* i *dccidd*. Budući da je *dd* alat napravljen za Linux operativne sustave, često je uključen u Android

platforme. To znači da metoda za stvaranje slike na uređaju često već postoji na uređaju i to je značajna pogodnost za osobu koja treba odraditi analizu mobilnog uređaja.

Naredba *dd* ima mnogo opcija koje se mogu postaviti, ali prezentirane će biti samo one forenzički bitne.

Sintaksa same naredbe izgleda ovako:

```
dd if=/dev/block/mmcblk0 of= /sdcard/blk0.img bs=4096
conv=notrunc,noerror,sync
```

Gdje je značenje pojedinog parametra:

- if: određuje ulaznu datoteku iz koje treba čitati.
- of: određuje izlaznu datoteku u koju treba pisati.
- bs: veličina bloka, podaci se čitaju i pišu u veličini navedenog bloka i zadane vrijednosti 512 bajta, ako nije drugačije navedeno
- conv: opcije pretvorbe:
- notrunc: ne skraćuje izlaznu datoteku.
- noerror: nastavlja snimanje ako se pojavi pogreška.
- sync: zajedno bez pogreške, ovo piše \x00 za blokove s greškom - ovo je važno za održavanje lokacija datoteka unutar slike

Da bi forenzičar mogao odrediti od koje particije će raditi sliku mora najprije stanje particija i ono što mu je prioritet, te gdje će sliku particije spremiti. Prvi korak je pokretanje ADB ljuske, a nakon toga naredbe `cat /proc/partitions`, da bi dobio ispis svih particija datotečnog sustava Većina particija vjerojatno neće biti forenzično zanimljiva, a da bi vidjeli odgovarajuća imena za svaku particiju i mogli identificirati one koje su nam važne, potrebno je potražiti popis imena particija. Za neke uređaje nalazi se na putanji `/dev/block/msm_sdcc.1/by-name`. Kretanjem do tog direktorija i izvršavanjem naredbe `ls –al` moguće je vidjeti gdje je svaki blok simbolično povezan. Kada znamo što je za našu istragu bitno, tj koja nas particija zanima i ako je za našu istragu zanimljiva samo particija s podacima o korisničkim podacima, sada znamo koja je to particija pa njezin identifikator treba koristiti kao ulaznu datoteku u naredbu *dd*. Ako mapa po imenu ne postoji na uređaju, možda neće biti moguće identificirati svaku particiju na uređaju. Međutim, mnogi od njih se još uvijek mogu pronaći pomoću naredbe *mount* unutar ADB ljuske.

Po identifikaciji podataka particije koju želimo analizirati možemo kreirati izlaznu datoteku na SD karticu uređaja. Na novijim uređajima `/sdcard` particija je zapravo simbolična veza

s mapom `/data/sdcard`. Najlakše je to utvrditi tako da pokrenemo ADB shell i pokrenemo naredbu `ls -al`. Kada odredimo što trebamo kopirati i gdje je točno SD kartica sliku podataka kreiramo naredbom

```
dd if=/dev/block/mmcblk0p28 of=/sdcard/data.img bs=512 conv=notrunc, noerror, sync
```[14]

Tako kreiranu sliku dalje možemo analizirati željenim alatom.

4.3.2. Fizička ekstrakcija podataka nand alatom

Aktualne verzije Android mobilnih uređaja imaju particije koje se sastoje od MMC blokova, dok se stariji uređaji sastoje od blokova memorijske tehnologije MTD (engl *Memory Technology Device*). Ukoliko se u toku forenzičkog postupka dogodi da *dd* ne može uspješno izraditi sliku MTD particije ili bloka potrebno je potražiti drugo rješenje. To drugo rješenje temelji se na jako rasprostranjenom alatu *MTD Utils*. Taj alat može čitati i pisati MTD blokove, a dio alata koji to obavlja zove se *nanddump* i može se koristiti isto kao i *dd* alat, ali sa svojstvom da uspješno čita MTD blokove. Verzije *nanddump* alata za Android dostupne su za preuzimanje sa internet, npr na poveznici https://github.com/jakev/android-binaries/blob/master/nanddump.

4.3.3. Fizička ekstrakcija podataka ACQUIRE alatom

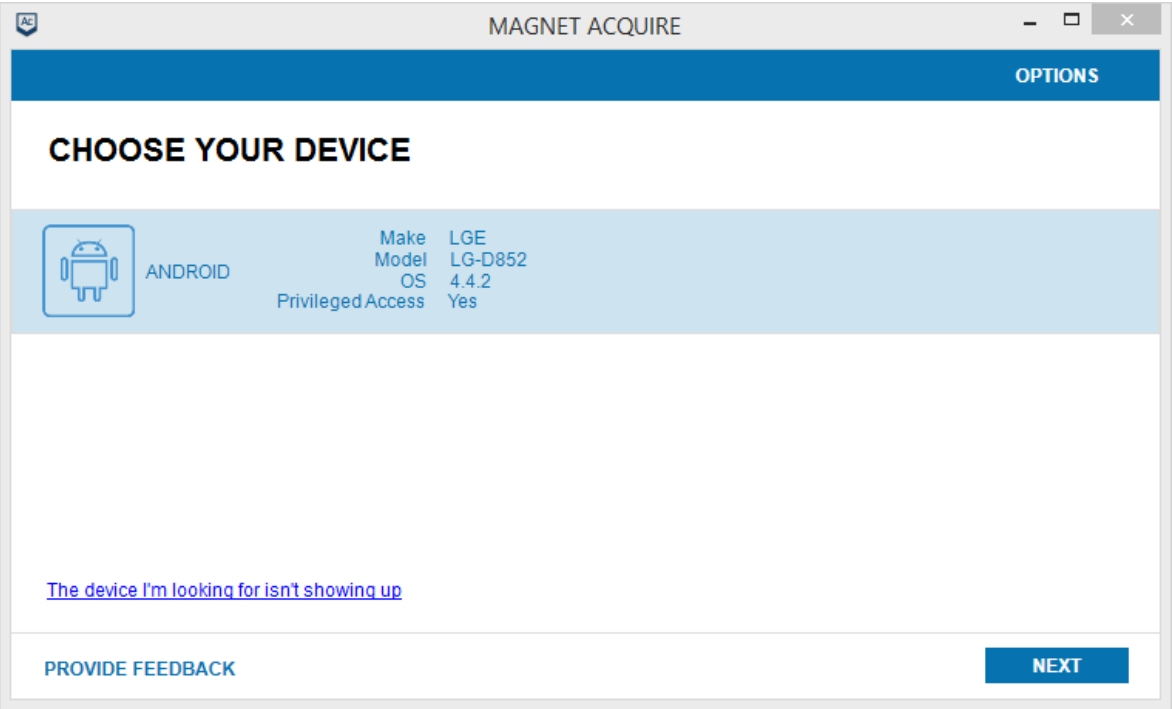
Alat tvrtke Magnet komercijalnog naziva ACQUIRE zamišljen je za brzo kreiranje slike bilo kojeg iOS ili Android uređaja i to na dva načina[15]:

- Brza ekstrakcija - radi sa bilo kojim iOS uređajem novijim od verzije 5, no ono što je zanimljivije je brza ekstrakcija slike Android uređaja, koja će sadržavati i sigurnosnu kopiju ADB-a, kao i dodatnu ekstrakciju povijesti pregledavanja internet preglednika i podataka nativnih aplikacija, na verzijama Androida novijima od verzije 2.1.
- Potpuna ekstrakcija - opcija koja radi potpunu sliku, fizičku sliku Android uređaja korištenjem ugrađenih mogućnosti eskalacije privilegija ili izradom slike uređaja na kojem je omogućen *root* pristup.

[14] https://resources.infosecinstitute.com/practical-android-phone-forensics/#gref (30.08.2019)
[15] https://www.magnetforensics.com/resources/image-smartphone-magnet-acquire/ (30.08.2019).

Upotreba aplikacije je jednostavna i za manje iskusne korisnike, budući da se odmah po priključenja na računalo sa instaliranom aplikacijom pokaže popis uređaja koji su povezani sa računalom forenzičara.

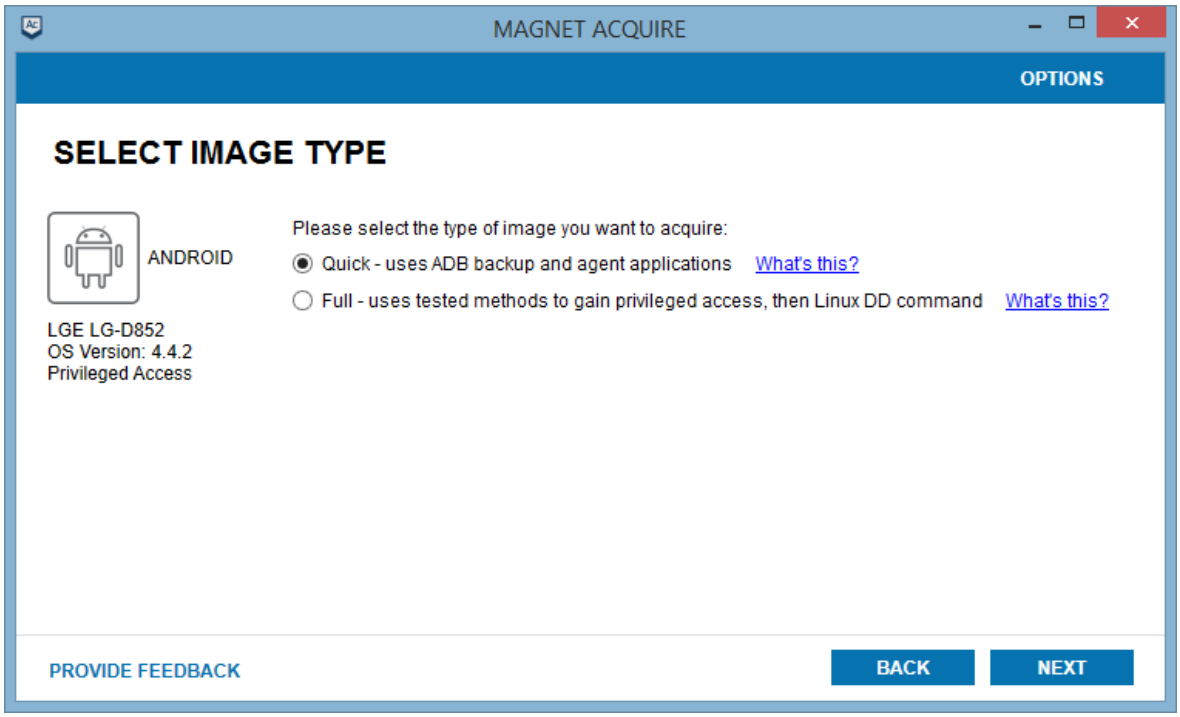
Preduvjet za funkcioniranje alata je ispravno instalirani upravljački programi za uređaj čiju sliku treba izraditi. Za Android uređaje Windows će pokušati instalirati upravljačke programe automatski, ali oni su često pogrešni i neće omogućiti podatkovnu vezu između računala i uređaja. Ukoliko se radi o operativnom sustavu Windows 8 ili novijem, na računalu forenzičara, da bi povezivanje bilo uspješno potrebno je preuzeti prilagođeni upravljački program tvrtke *Magnet Forensics*, kako bi povezivanje bilo uspješno.



Slika 4.4 Priključeni uređaj na aplikaciju Magnet Acquire[16]

Kako prikazuje Slika 4.4 Priključeni uređaj na aplikaciju Magnet Acquire vidi se da je priključeni uređaj LG-D852 (komercijalnog naziva LG G3). Nakon što ACQUIRE uspješno detektira uređaj na njemu mora biti omogućeno USB otklanjanje grešaka i da je na mobilnom uređaju omogućen pristup s računala. Nakon što se veza uspješno uspostavi potrebno je odabrati način izrade slike – brza ili puna ekstrakcija; Slika 4.5 Odabir vrste ekstrakcije.

[16] https://www.magnetforensics.com/resources/image-smartphone-magnet-acquire/ (17.08.2019.)

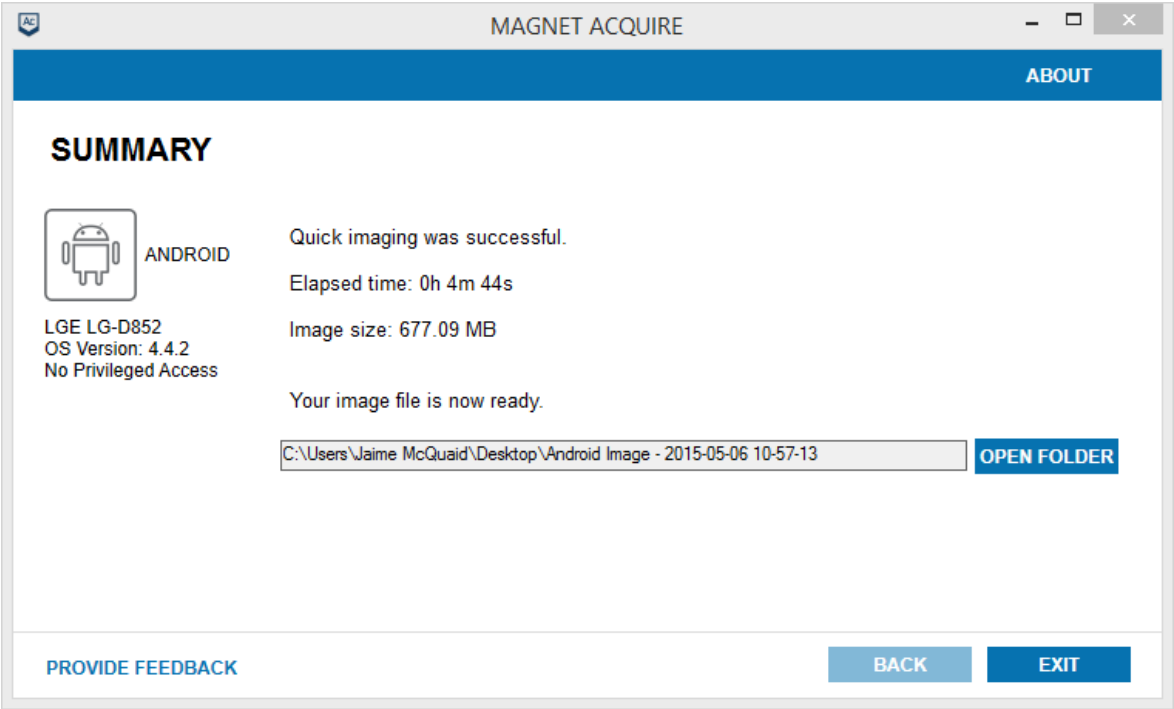


Slika 4.5 Odabir vrste ekstrakcije[17]

Brza ekstrakcija djelovat će na bilo kojem uređaju, što će omogućiti stjecanje vrijednih podataka aplikacija proizvođača uređaja, ali i aplikacija trećih strana na uređaju. Brza ekstrakcija forenzičaru će ispisati obavijest ima li uređaj vrijedne podatke koji su vrijedni dodatnog vremena i trud više ručnih tehnika. Ako su potrebni dodatni podaci, često se kao alternativa koristi JTAG ili izdvajanje čipova.

Kada završi izrada slike ACQUIRE alatom otvorit će se dijaloški okvir sa informacijama o načinu izrade slike, trajanju izrade, veličini slike i njenoj lokaciji .

[17] https://www.magnetforensics.com/resources/image-smartphone-magnet-acquire/ (17.08.2019.)

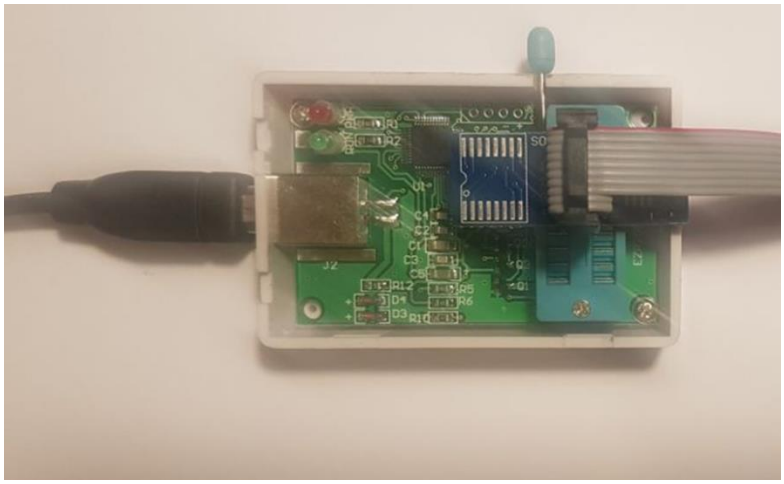


Slika 4.6 Završetak izrade slike mobilnog uređaja[18]

4.3.4. JTAG ekstrakcija

JTAG, (engl. *Joint Test Action Group*) je standard donesen od strane Institute of Electrical and Electronics Engineers (IEEE). JTAG se prvotno koristio za za komunikaciju sa procesorom u elektroničkim uređajima, pomoću JTAG programatora ili interfejsa Slika 4.7 JTAG programator, u svrhu testiranja i otklanjanja nedostataka putem specijaliziranog sučelja i protokola.

[18] https://www.magnetforensics.com/resources/image-smartphone-magnet-acquire/ (17.08.2019.)



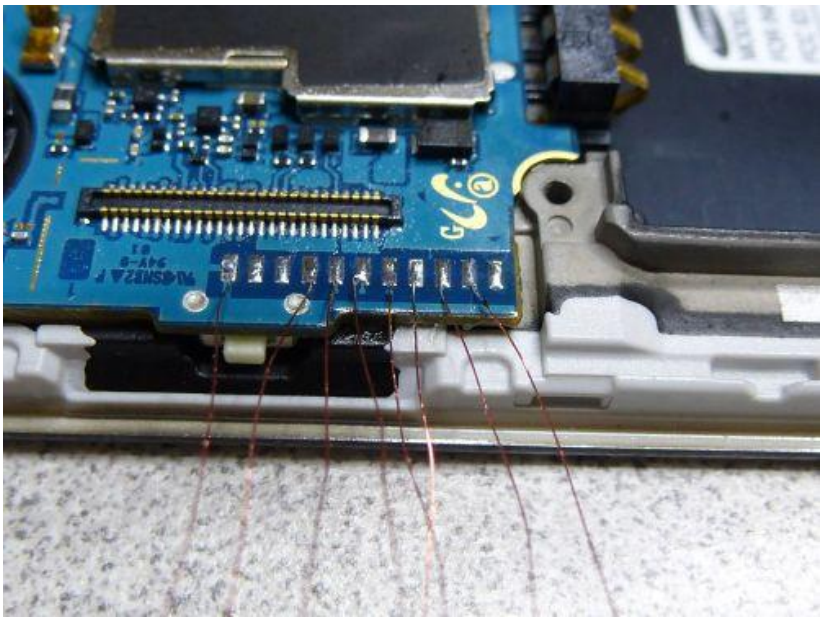
Slika 4.7 JTAG programator[19]

To sučelje na mobilnim uređajima omogućava komunikaciju izravno sa procesorom i dohvat pune fizičke slike flash memorije. Da bi se to omogućilo potrebno je rastaviti uređaj i znati raspored priključaka Slika 4.8 JTAG sučelje mobilnog uređaja.

Slika 4.8 JTAG sučelje mobilnog uređaja[20]

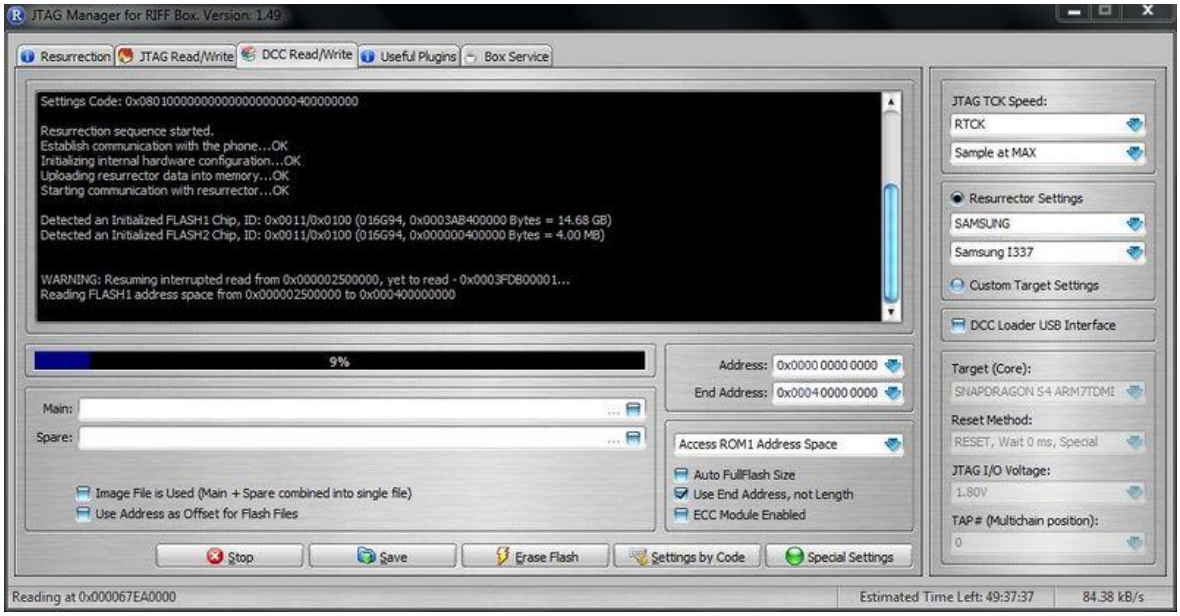
Obično je za većinu uređaja taj podatak moguće naći na internetu ili u servisnim dokumentacijama. Od drugih pomagala trebamo JTAG programator i odgovarajuću JTAG aplikaciju. Kada rastavimo uređaj i znamo raspored pinova JTAG priključka, te priključimo JTAG sučelje mobilnog uređaja sa JTAG programatorom.

[19] Vlastita slika autora (14.09.2019.)
[20] https://forensicswiki.org/wiki/JTAG_Samsung_Galaxy_S4_(SGH-I337) (30.08.2019.)



Slika 4.9 Mobilni uređaj priključen na JTAG programator[21]

zatim mobilni uređaj priključimo na izvor napajanja, a programator na računalo forenzičara i spremni smo za pokretanje aplikacije.



Slika 4.10 JTAG aplikacija[22]

Tada treba biti pokrenuta JTAG aplikacija, konfigurirana, spojena sa mobilnim uređajem i uključen mobilni uređaj tipkom za uključivanje. Nakon uključivanja mobilnog uređaja treba pokrenuti "PROČITAJ" na kartici "Čitanje/pisanje u DCC-u". Ako sve pođe dobro, gumb

[21] https://forensicswiki.org/wiki/JTAG_Samsung_Galaxy_S4_(SGH-I337) (30.08.2019.)
[22] https://forensicswiki.org/wiki/JTAG_Samsung_Galaxy_S4_(SGH-I337) (30.08.2019.)

"PROČITAJ" postat će tipka "STOP" i telefon će početi čitati, a ako ne, softver pruža korake za rješavanje problema koje treba poduzeti kako bi pomogli u dijagnosticiranju problema koji se mogu pojaviti. U slučaju pogreške čitanja softver prati mjesto na kojem je došlo do prekida u čitanju i daje vam mogućnost ponovnog pokretanja čitanja tamo gdje je stao. Kada je kreiranje slike dovršeno, ona se može spremiti i na njoj se može vršiti forenzička analiza pomoću odabranog alata.

4.3.5. Odlemljivanje čipova

Chip-off je zadnja metoda ekstrakcije podataka koja nam je na raspolaganju i ona je destruktivna budući da se u njoj memorijski čip odlemljuje iz mobilnog uređaja. Najčešće se postupak izvodi vrućim zrakom uz kontroliranu temperaturu, kako ne bi došlo do pregrijavanja i trajnog oštećenja memorijskog čipa. Temperatura zraka mora biti takva da se čip odlemi, tj da se odvoji od matične pločice i obično iznosi oko 200 do 230 °C. Tako skinuti čip priključuje se na specijalna podnožja, koje mora odgovarati svakom pojedinom memorijskom čipu. Znajući da je je broj modela praktički nebrojiv na tržištu toliko forenzičar treba imati različitih adaptera. Pomoću tog adaptera postavlja se na programator, koji onda pak radi sliku cijele memorije čipa i ta slika se dalje može analizirati. Razlika između JTAG metode i chip-off je u tome što kod JTAG-a uređaj mora bit uključen i priključen na programator, a kod chip-off-a imamo samo memorijski čip priključen na programator. Uz programator moramo imati lemnu stanicu sa vrućim zrakom i programsku podršku za programator, kao na primjer, Dataman 48Pro2 Super Fast Universal ISP Programmer kako bi mogli izradi sliku memorije.

Slika 4.11 Dataman 48Pro2 Super Fast Universal ISP Programmer[23]

[23]https://www.dataman.com/programmers/universal/dataman-48pro2-super-fast-universal-isp-programmer.html (01.09.2019)

5. Povrat obrisanih podataka

Povrat obrisanih podataka jedan je od najvažnijih aspekata forenzike mobilnih uređaja, jer se radi o ekstrakciji podataka kojima se više ne može pristupiti putem korisničkog sučelja. Povrat obrisanih podataka može imati primjenu u raznim slučajevima od privatnih, poslovnih, pa do rješavanja građanskih ili kaznenih slučajeva. To se pogotovo odnosi na slučajeve kada pojedinac ili skupina obrišu podatke sa svojih uređaja kako bi prikrili neku radnju ili djelo. Promatrajući proces povrata obrisanih podataka očima privatnog korisnika, može se raditi o greškom obrisanim slikama bliskih osoba ili obitelji. Ono što bi takvim korisnicima bilo najjednostavnije za upotrebu je koš za smeće kao što to ima operativni sustav Windows za računala. Takva funkcionalnost pojavila se i u sustavu Android od verzije 9.0 (engl. *Pie*) i galerija slika ima "smeće" odakle se obrisane stavke mogu jednostavno vratiti na originalnu lokaciju od strane samog korisnika.

No uz sve te funkcionalnosti postoji i tehnike povrata obrisanih podataka koje nisu dostupne običnim korisnicima, a omogućuju forenzičarima povrat obrisanih podataka. Promatrajući Android sa forenzičkog stajališta moguće je izvršiti povrat većine izbrisanih podataka, uključujući SMS poruke, slike, podatke o korištenim aplikacijama itd. Da bi forenzički postupak bio uspješan važno je slijediti korake forenzičkog postupka, što znači pravilno oduzimanje i svih koraka dalje u postupku kako ne bi došlo do nehotičnog postupka oštećenja ili uništenja forenzičkih tragova. Važno je imati na umu da su obrisani podaci u memoriji mobilnog uređaja, identično kao i na čvrstom disku računala, tako dugo dok na njihovo mjesto uređaj ne zapiše neki drugi podatak. To ne mora biti namjerno zapisivanje, nego na primjer može doći nova poruka elektroničke pošte u dolazni pretinac i prebrisati neku postojeću. Ono što je važno imati na umu je spomenuta mogućnost udaljenog brisanja.

Govoreći o povratu izbrisanih podataka sa mobilnog uređaja; kada korisnik izbriše bilo koje podatke s uređaja, podaci se zapravo ne brišu s uređaja i nastavljaju postojati na njemu. Dogodi se isti proces kao i kada se podatak obriše na mehaničkom čvrstom disku računala, izbriše se samo pokazivač na podatke. Svi datotečni sustavi sadrže meta podatke koji održavaju informacije o hijerarhiji datoteka, naziva datoteka itd. Brisanje neće stvarno izbrisati podatke, već umjesto toga uklanja meta podatke datotečnog sustava. Dakle, kad se tekstualne poruke ili bilo koje druge datoteke brišu s uređaja, njima se zapravo mijenja atribut i postaju nevidljive za korisnika, ali podaci su i dalje prisutni na uređaju sve dok nisu

prepisani nekim drugim podacima. Stoga postoji mogućnost da ih se obnovi prije nego što se novi podaci zapišu na njihovo mjesto, nebitno o kojem tipu podataka se radi. Cijeli proces brisanja podataka tako funkcionira jer je brisanje pokazivača i označavanje prostora kao dostupnog izuzetno brz proces u odnosu na stvarno brisanje svih podataka s uređaja. Stoga, radi povećanja performansi, i rada sa memorijom, operativni sustavi samo brišu meta podate.

Povrat podataka moguć je sa nekoliko mjesta spremanja, a tu spadaju:

- SD kartice - na njih se najčešće pohranjuju slike i videozapisi
- SQLite - u baze se spremaju poruke, povijest lokacija, poruke elektroničke pošte i slično
- Interna memorija uređaja - može sadržavati bilo koji tip podatka

5.1. Oporavak podataka sa SD kartica

Glavni podaci koji se spremaju na SD kartici su video zapisi i slike. No na novijim verzijama Androida na SD karticu mogu se instalirati i same aplikacije tako da se na SD kartici može otkriti mnoštvo informacija koje su korisne tijekom forenzičke istraga. Činjenica da su slike, videozapisi, glasovni snimci i podaci o aplikaciji pohranjeni na SD kartici tome dodaju težinu. Kao što je spomenuto u prethodnim poglavljima, Android uređaji često koriste datotečne sustave FAT32 ili exFAT na SD kartici, tako da je obnavljanje podataka izbrisanih s vanjskog SD-a prilično jednostavno ako se kartica može montirati kao pogon na računalu. Pošto je SD kartica uklonjiva, nju se može montirati kao pogon povezivanjem s računalom pomoću čitača kartica. Neki od starijih Android uređaja koji koriste USB masovnu pohranu dodjeljuju mobilnom uređaju slovnu oznaku pogona kada se spojeni putem USB kabela. Kako je ranije objašnjeno, da bismo bili sigurni da izvorni dokazi nisu modificirani, uzima se fizička slika diska i sve daljnje eksperimentiranje provodi se na samoj slici. Tako je i u slučaju SD kartice, potrebno je napraviti sliku SD kartice. U našem primjeru korišten je *FTK Imager*[24] tvrtke AccessData, koji namijenjen za izradu slika digitalnih medija. Uz stvaranje slike medija, može biti korišten i za istraživanje sadržaja slike diska.

[24] https://accessdata.com/product-download/ftk-imager-version-3-2-0 (10.09.2019.)

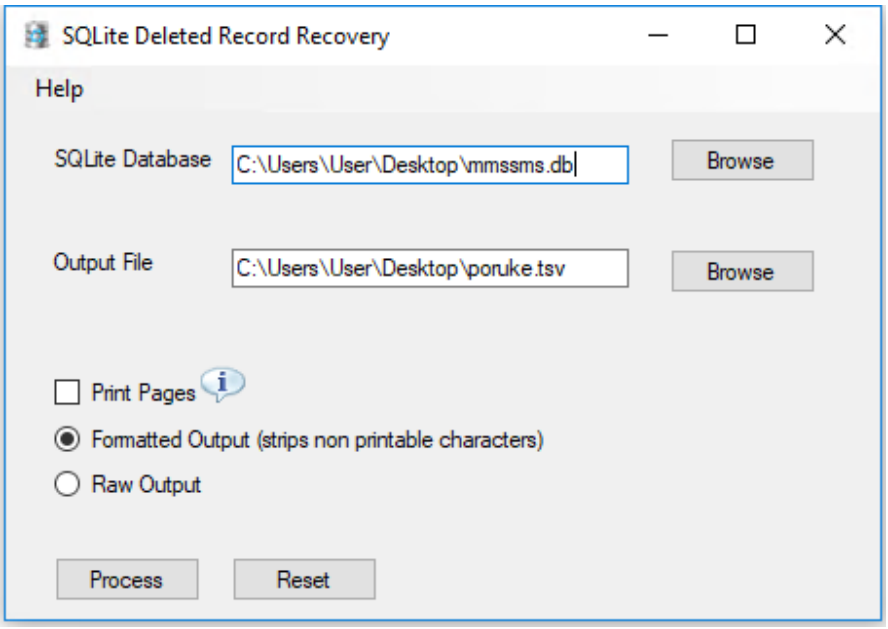
5.2. Oporavak izbrisanih zapisa iz SQLitea baze podataka

Većina podataka Android aplikacija pohranjena je u bazama podataka SQLite. Podaci koji se odnose na tekst poruke, poruke elektroničke pošte, a i većina podataka o aplikacijama elektroničke pošte pohranjuju se u isto takve baze podataka. Te baze podataka također u sebi mogu sadržavati podatke za brisanje. Zapisi označeni za brisanje od strane korisnika ne pojavljuju se u aktivnim datotekama SQLite baze podataka. Stoga je moguće izvršiti povrat tih podataka analizom tih datoteka. Unutar SQLite tablica postoje dva područja koja mogu sadržavati obrisane podatke - nedodijeljeni blokovi i slobodni blokovi. Većina komercijalnih forenzičkih alata upravo i skenira ta dva područja. Ekstrakcija takvih podataka može se vršiti alatima poput *Belkasoft Evidence Center*[25] i on je dostupan u probnoj verziji za slobodno preuzimanje.

Ako uzmemo za primjer vraćanje izbrisanih SMS poruka s Android telefona što se često traži kao dio forenzičke analize na uređaju. SMS poruke nalaze se u mmssms.db, SQLite bazu podataka koja sadrži SMS poruke poslane ili primljene pomoću aplikacije Android Messages.

Ova se baza podataka nalazi u mapi data/com.android.providers.telephony/databases/. Nakon što imamo fizičku sliku uređaja bazu možemo izvući pomoću FTK Imagera, baš kao što je to slučaj s izbrisanim datotekama. Najlakši način za pronalaženje izbrisanih zapisa je uporaba komercijalnih mobilnih forenzičkih alata, kao što su *Belkasoft Evidence Center*, *Cellebrite UFED Physical Analyzer*[26], *Oxygen Forensic Detective*[27], itd. No postoje i alati otvorenog koda koji mogu ekstrahirati podatke, nedodijeljeni prostor i drugo. Jedan od takvih alata je *SQLite Deleted Records Parser*[28]. Ovaj GUI alat ima intuitivno sučelje u kojem je potrebno odabrati izvorišnu bazu i odredišnu datoteku u koju će spremiti željene podatke iz baze, u ovom slučaju SMS poruke.

[25] https://belkasoft.com/ec (10.09.2019.)
[26] https://www.cellebrite.com/en/ufed-ultimate/ (10.09.2019)
[27] https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective (10.09.2019.)
[28] https://github.com/mdegrazia/SQLite-Deleted-Records-Parser/blob/master/sqlparse_GUI_1_3.zip (11.09.2019.)



Slika 5.1 SQLite Deleted Record Recovery[29]

5.3. Oporavak podataka iz interne memorije

Ekstrakcija izbrisanih datoteka iz interne memorije Android mobilnog uređaja nije jednostavno kao ekstrakcija iz SQLite baze podataka ili SD kartice, ali je izvedivo. Postoji više komercijalnih alata koji mogu vratiti i ekstrahirati obrisane podatke ukoliko memorija uređaja i particija s podacima nisu šifrirani. No srećom za forenzičare to baš nije česta pojava kod korisnika, posebno na novijim verzijama Android operativnog sustava u verzijama kao što su Oreo i Pie.

Većina Android uređaja, posebno modernih pametnih telefona i tableta, koristi datotečni sustav EXT4 za organiziranje podataka u njihovu unutarnju pohranu. Ovaj je datotečni sustav vrlo uobičajen za Linux operativne sustave. Dakle, ako je zahtjev vratiti izbrisane podatke iz interne memorije uređaja, potreban je alat koji to može odraditi sa datotečnog sustava EXT4. Primjer takvog alata je Extundelete[30]

Za upotrebu ovog alata potrebna je Linux radna stanica. Većina Linux forenzičkih distribucija već ima instaliran taj alat, uz mnoge druge. Primjer takve Linux forenzičke

[29] Vlastita slika zaslona računala autora (12.09.2019.
[30] http://extundelete.sourceforge.net/ (10.08.2019.)

distribucije je SIFT Workstation[31] koje se koristi i na Visokom učilištu Algebra. Radi se o Linux distribuciji za računalnu forenziku i odgovaranje na incidente, kreirane na SANS Institutu (engl. *Escal Institute of Advanced Technologies*) i može se preuzeti sa poveznice https://digital-forensics.sans.org/community/downloads

Nakon pokretanja alata naredbom

```
extundelete --help
```

vidi se ispis svih opcija alata

Da se može razlučiti lokacija korisničkih podataka unutar slike memorije uređaja koristi se naredba sintakse:

```
mmls <ime slike> iz Sleuth Kit-a
```

na rezultatu potrebno je identificirati particiju sa opisom userdata

da bi uvjerili da je particija stvarno ext4 formata služi naredba

```
fsstat -o xxxxxxx <ime slike>
```

gdje je xxxxxxx početni sektor userdata particije. Sve što sada još treba je montirati particiju userdata i pokrenuti naredbu *extundelete* u obliku

```
extundelete /userdata/partition/mount/point --restore-all
```

Sve ekstrahirane datoteke bit će spremljene u poddirektoriju trenutnog naziva RECOVERED_FILES.

[31] https://digital-forensics.sans.org/community/downloads (18.06.2019.)

6. Alati za forenzičku analizu Android platforme

6.1. EnCase Mobile Investigator

EnCase Mobile Investigator[32] je produkt tvrtke EnCase koja je lider na području računalne forenzike, a EnCase Mobile Investigator je namijenjen za intuitivno pregledavanje, analiziranje, označavanje i prijave svih mobilnih dokaza relevantnih za sve forenzičke slučajeve u jednom produktu. Dizajniran kako bi poboljšao način na koji istražitelji pregledavaju kritične dokaze o mobilnim uređajima. Aplikacija je prema tvrdnji proizvođača, izgrađena s dubokim razumijevanjem integriteta dokaza, tako da je moguće nesmetano dovršiti svaku istragu, uz podršku dokaza, u rasponu od tekstualnih poruka, zapisa poziva, fotografija, pa do podataka aplikacija. EnCase Mobile Investigator omogućava istražiteljima da rade na slučaju neprimjetno, temeljito i učinkovito.

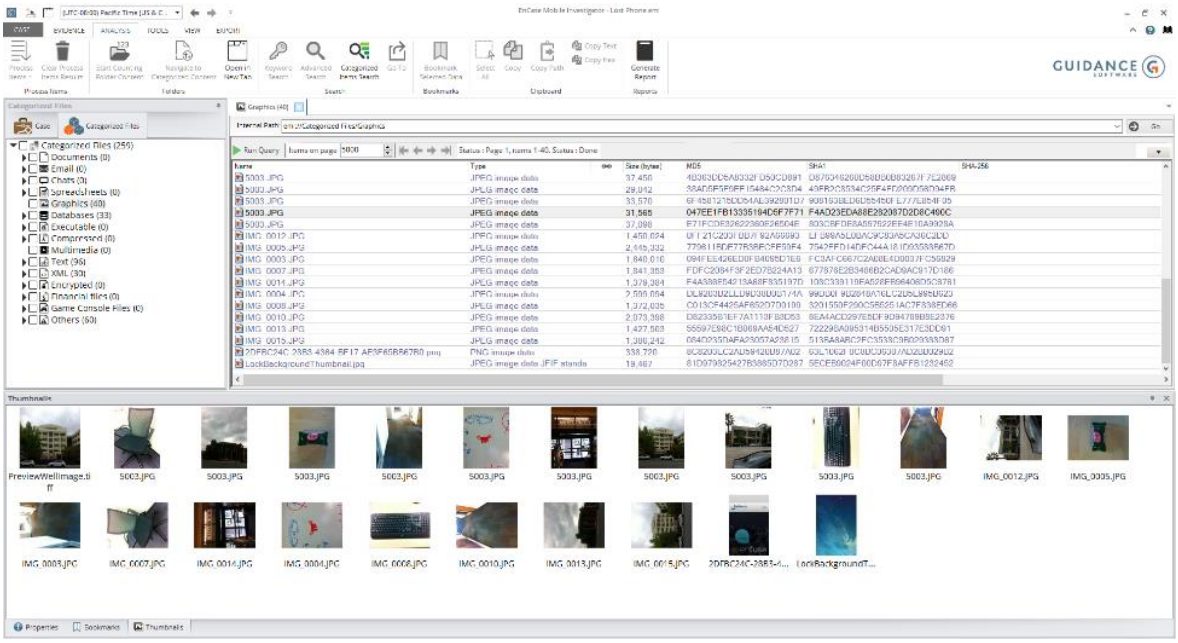
Ključne prednosti:

- Intuitivni pregled dokaza - S EnCase Mobile Investigatorom forenzičari lako mogu pregledavati raščlanjene dokaze mobilnih uređaja iz najšireg spektra mobilnih aplikacija, uključujući tekstualne poruke, e-mailove, zapise poziva, spremišta podataka u oblaku povezane s mobilnim uređajima, povijest pregledavanja internetskih preglednika, fotografije, podatke o aplikacijama i izbrisane podatke.
- Stalna podrška - Istražitelji trebaju pouzdano forenzičko rješenje koje mogu koristiti kada je u pitanju bilo koja istraga koja uključuje mobilni uređaj. Uz česte nadogradnje operativnog sustava i ažuriranja aplikacija u *EnCase Mobile Investigator*-u, ispitivači mogu držati korak s stalnom evolucijom mobilnih uređaja i mobilnih aplikacije koje se stalno nadograđuju novim funkcionalnostima.
- Vrhunski pristup - Postoje mnogi mobilni uređaji s kojima se suočavaju istražitelji da su zaključani ili zaštićeni lozinkom. EnCase Mobile Investigator omogućuje istražitelju nudeći nekoliko ugrađenih zaobići funkcije zaključavanja tako da nema dokaza unutar uređaja koji može biti sakriven i ne može mu pristupiti.
- Sveobuhvatna podrška tipova podataka - Sa *EnCase Mobile Investigator*-om, obuhvaćeni su svi tipovi ulaznih podataka poput SQLite, Pliste, arhive, PDF, HTML

[32] https://www.sans.org/reading-room/whitepapers/analyst/membership/38490 (10.09.2019.)

i ostali koristeći značajku univerzalnog preglednika datoteka. Forenzičarima to omogućuje da prikupe najširi spektar dokaza potrebnih za njihovu istragu, uključujući sve podatke povezane s velikim brojem aplikacija.

- OCR visoke kvalitete - *EnCase Mobile Investigator* omogućuje forenzičarima da pronađu, izdvoje i analiziraju podatke u grafičkim datotekama koristeći optičko prepoznavanje znakova (engl. OCR - Optical Character Recognition). Tu spadaju dokazi iz grafičkih datoteka poput PDF-a, fotografije i druge vrste datoteka u kojima se pronađu rezultati pokretanja pretraživanja ključnih riječi, osiguravajući otkrivanje kritičnih dokazi bez obzira na to kako su pohranjeni.
- Snažna vidljivost aplikacija u oblaku - Prikupljanje podataka iz aplikacija društvenih mreža i izvori podataka u oblaku koji mogu biti povezani s mobilnim uređajem i mogu biti presudni za istragu kojom će se dokazati osumnjičenikova krivnja ili nevinost. Uz odgovarajuća dopuštenja, istražitelji mogu koristiti EnCase Mobile Investigator za prikupiljanje i pregled dokaza osumnjičenih iz korisničkih računa u oblaku poput Google Diska, Twittera, Facebooka i drugih. Ova moćna značajka poboljšava i proširuje sposobnosti kojima raspolažu istražitelji.
- Robusna pretraga - Dok istražitelji pronalaze dokaze, svaki trag koji se pojavi, dodatno se analizira i prati još dublje. Vrsta pretrage dokaza uključena u *EnCase Mobile Investigator* omogućuje istražiteljima da mogu locirati kreditne kartice, adrese elektroničke pošte i brojeve telefona kako bi pronašli dodatne dokaze koji bi pomogli dovršiti njihovu forenzičku analizu i postići što bolje rezultate.
- Pojednostavljeno stvaranje izvješća - Nakon što se prikupe svi relevantni dokazi, istražitelji mogu stvoriti intuitivno izvješće. Postoji nekoliko prilagodljivih mogućnosti izvještavanja koje se nude s EnCase Mobile Investigator-om uključujući HTML, vremenski slijed, PDF i mnoge druge varijacije izvještaja. Ova izvješća su kreirana da se mogu lako podijeliti i da na uvjerljiv i jednostavan načina za čitanje prezentiraju rezultate svake analize.



Slika 6.1 EnCase Mobile Investigator[33]

6.2. UFED Ultimate

Kompliciranе sigurnosne mjere poput zaključavanja mobilnih uređaja, enkripcijskih barijera, obrisani ili nepoznati sadržaji i ostale prepreke forenzičkoj analitici podataka mobilnih uređaja kao što su pregledavanje javnih socijalnih medija i podaci u cloud servisima mogu sprečavati prikupljanje dokaza. Kako bi istraga dobila najbolji mogući rezultat, forenzičari i istražitelji trebaju temeljito i brzo izvući forenzički ispravne podatke i pružiti smislene uvide koji bi to mogli učiniti i pomoći u napretku slučaja. *UFED Ultimate*[34] vodeće je tržišno rješenje za pristup digitalnim forenzičkim podacima s nenadmašnim mogućnostima izdvajanja i dekodiranja podataka iz najšireg raspona uređaja i aplikacija. Detaljno istraživanje sa sveobuhvatnim pristupom logičkom, datotečnom sustavu i fizički izvađenim podacima, čak i skrivenim i izbrisanim, i otkrivanje kritičnih dokaza koji može riješiti slučaj cilj je UFED produkta.

[33] https://www.guidancesoftware.com/blog/digital-forensics/2017/07/05/three-things-you-need-to-know-about-encase-mobile-investigator (28.08.2019.)

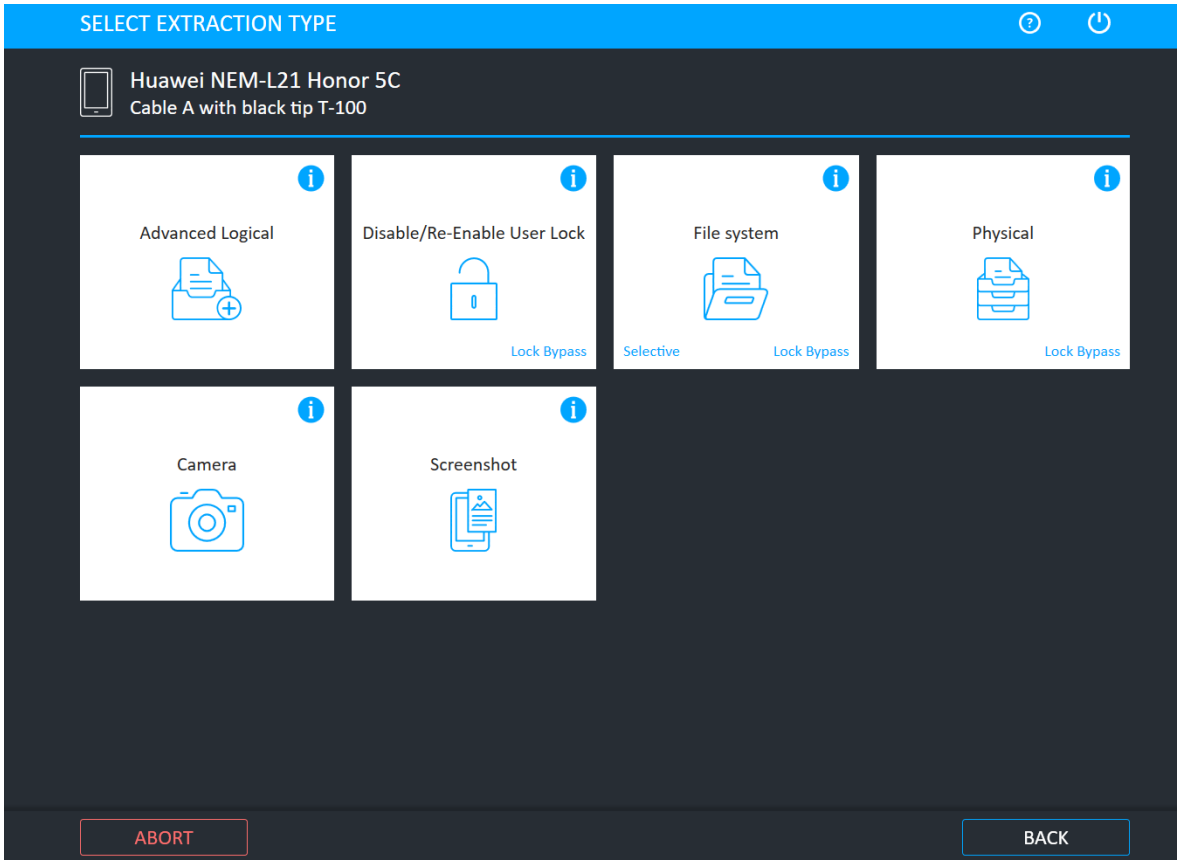
[34] https://cf-media.cellebrite.com/wp-content/uploads/2017/05/DataSheet_UFEDUltimate_A4_2019_web.pdf (28.08.2019.)

Ovaj robustan i učinkovit alat također pomaže objediniti prikupljene podatke i pregledati ih brže te lako dijeljenje nalaza sa cijelim istražnim timom, čak i onima koji ne koriste Cellebrite proizvode. Osigurava ostanak u grupi vodećih lidera po mogućnostima digitalnog forenzičkog ispitivanja s najnovijom tehnologijom i podrškom za različite hardverske platforme. UFED Ultimate pruža maksimalan pristup podacima koji su potrebni za izgradnju jakih, obrambenih slučajeva.

Ključne prednosti:

- Oporavlja najviše podataka s većine uređaja i aplikacija.
- Otključava uređaje s lakoćom - Zaobilazi obrazac, zaključavanje lozinkom ili PIN-om i nadjačava izazove šifriranja brzo i jednostavno pružajući svom timu pristup ekstrakciji i brzoj analizi sadržaja
- Detaljno istražuje i izvlači mnogo podataka - Izvodi forenzički napredni logički, datotečni sustav i fizičko izdvajanja netaknutih, skrivenih i izbrisanih podataka. Novi *bootloader*-i, mogućnosti automatskog EDL-a, pametni ADB i druge metode ekstrakcije omogućuju pristup podacima najširem rasponu uređaja, uključujući pametne telefone, tablete, GPS uređaje, pametni satove i još mnogo toga.
- Sveobuhvatno i brzo dešifriranje - Omogućuje rekonstrukciju podataka uređaja i aplikacija u čitljive formate s naprednim mogućnostima dekodiranja, kao što su Python skripte i heksadecimalna analiza. Izdvaja nedodijeljeni prostor u memoriji uređaja za ekstrakciju izbrisanih podataka i medijskih sadržaja. Otkriva nove i skrivene izvore podataka pomoću *SQLite Data Wizarda* i primjene metode algoritma slučajnog otkrivanja velike količine dokaza.
- Objedinjuje podatke za cjelovitiji pregled - Automatski objedinjuje podatke uređaja iz različitih izvora i formati u jedinstvenom prikazu. Omogućuje forenzičaru da usredotočuje svoju analizu na napredne alate za pretraživanje, filtriranje, označavanje, mape i vremenske podatke za utvrđivanje čvrstoća povezanosti ljudi, mjesta i događaja.
- Skraćuje vrijeme do dobivanja dokaza - Moguće je izravno uvesti nalaze iz *UFED Physical Analyzera* u *Analytics Desktop* u jednom pojednostavljenom tijeku rada za objedinjavanje podataka iz drugih digitalnih izvora i temeljito istražiti sve digitalne tragove koji su ostavljeni. Omogućuje dijeljenje nalaze s istražnim timom dinamičnim, prilagođenim izvještavanjem koje je moguće prilagoditi svakom specifičnom zahtjevu kolega za analizu.

- Ispitivanje dokaza je povoljno – Implementacija *UFED Ultimate* na ispravnoj platformi da podržava tijek rada i okolinu, omogućuje izbor između 4PC softvera koji je moguće instalirati na hardver po izboru ili ga povezati sa Touch2, pojačanom verzijomTouch2 ili pojačanim prijenosnim računalom za ekstrakcije na terenu.



Slika 6.2 UFED Ultimate[35]

6.3. Autopsy

Autopsy je besplatni alat za analizu otvorenog koda koji je u početku razvio Brian Carrier. Početak *Autopsy*[36]-ja je bio kao grafičko korisničko sučelje za *Linux Sleuth Kit*[37] temeljen na Linux skupu alata, ali od verzije 3, to je samostalni alat kreiran za Windows platformu. Alat nije namijenjen obavljanju akvizicija mobilnih uređaja, ali može analizirati većinu uobičajenih Android datoteke (poput YAFFS i EXT). *Autopsy* je digitalna forenzička

[35] https://www.cellebrite.com/en/ufed-ultimate/ (01.09.2019.)
[36] https://www.sleuthkit.org/autopsy/ (01.09.2019.)
[37] https://www.sleuthkit.org/(01.09.2019.)

platforma i grafičko sučelje za Sleuth Kit i druge digitalne alate za forenziku. Koriste ga forenzičari za provedbu zakona, vojska i korporacije kako bi istražili slijed događaja na računalu. Može se čak koristiti za ekstrakciju fotografija s memorijske kartice fotoaparata.

- Jednostavan je za korištenje zamišljen tako da se intuitivno i jednostavno obavi analitika. Instalacija je jednostavna, a čarobnjaci vode kroz svaki korak. Svi se rezultati nalaze u jednoj strukturi stabla.
- Proširiva platforma - *Autopsy* je osmišljen kao platforma s modulima koji dolaze izvan okvira same aplikacije i koji su dostupni kao produkti trećih strana.
- Brza analitika - Svi korisnici analitike žele rezultate što prije, a *Autopsy* paralelno izvodi pozadinske zadatke koristeći više jezgara i daje rezultate čim ih pronađe. Analiza može potrajati satima za potpuno pretraživanje slike, ali za nekoliko minuta daje podatke jesu li ključne riječi pronađene u korisničkoj slici mobilnog uređaja nad kojim se vrši analiza.
- Povoljno - *Autopsy* je besplatan proizvod. Kako se proračuni tvrtki smanjuju, ključna su ekonomična rješenja za digitalnu forenziku. Autopsy nudi iste temeljne funkcionalnosti kao i drugi alati za digitalnu forenziku čije su cijene visoke, ali i nudi druge bitne značajke, poput analize web artefakata i analize registra, koje drugi komercijalni alati čak i ne pružaju.
- Funkcionalnosti *Autopsy*-a ćemo prikazati u slijedećem poglavlju analiza slike uređaja.

7. Analiza preuzetih slika uređaja

7.1. Slika uređaja

Nacionalni institut za standarde i tehnologiju (engl. *National Institute of Standards and Technology - NIST*) laboratorij je fizičkih znanosti i ne regulirajuća agencija Ministarstva trgovine Sjedinjenih Država. Njegova misija je promicanje inovacija i industrijske konkurentnosti. Aktivnosti NIST-a organizirane su u laboratorijske programe koji uključuju znanost i tehnologiju, inženjering, informatičku tehnologiju, neutronska istraživanja, mjerenje materijala i fizičko mjerenje[38].

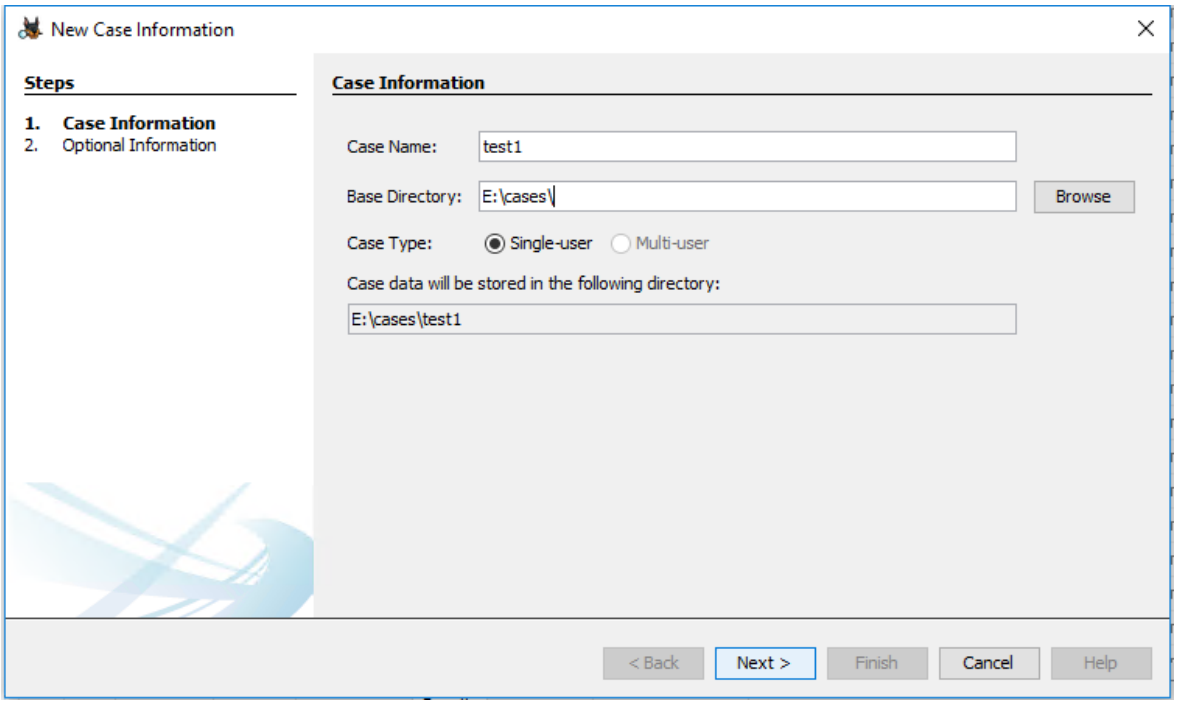
NIST u svojem portfelju ima razvijene računalne forenzičke skupove referentnih podataka (engl. *Computer Forensic Reference Data Sets - CFReDS*) za digitalne dokaze. Ovi skupovi podataka pružaju istražiteljima dokumentirane skupove simuliranih digitalnih dokaza za ispitivanje. Budući da CFReDS ima dokumentirani sadržaj, poput ciljnih nizova rezultata pozicioniranih na poznatim mjestima CFReDS-a, istražitelji mogu usporediti rezultate analiza sa poznatim rezultatima. Istražitelji mogu koristiti CFReDS na nekoliko načina, uključujući provjeru softverskog alata koji se koristi u njihovim analizama, provjeru opreme, obuku istražitelja i testiranje stručnosti istražitelja u sklopu akreditacije laboratorija. Na mjestu za preuzimanje CFReDS nalazi se više referentnih slika i rezultati analiza. Neke slike izrađuje NIST, često iz projekta CFTT (engl. Computer Forensic tool testing), a neke daju druge organizacije. Nacionalni institut za pravosuđe dijelom je financirao ovaj rad putem međuagencijskog sporazuma s Uredom za provedbu zakona *NIST*-a.

Slika korištena za analizu alatom *Autopsy* preuzeta je sa stranice *NIST*-a sa poveznice https://www.cfreds.nist.gov/mobile/index.html odakle je preuzet i dokument *Mobile Device Data Population_samsungGalaxyS4_N116133* gdje su opisani nalazi koji se nalaze u slici sustava ekstrahiranoj JTAG postupkom.

[38] https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology (22.05.2019.)

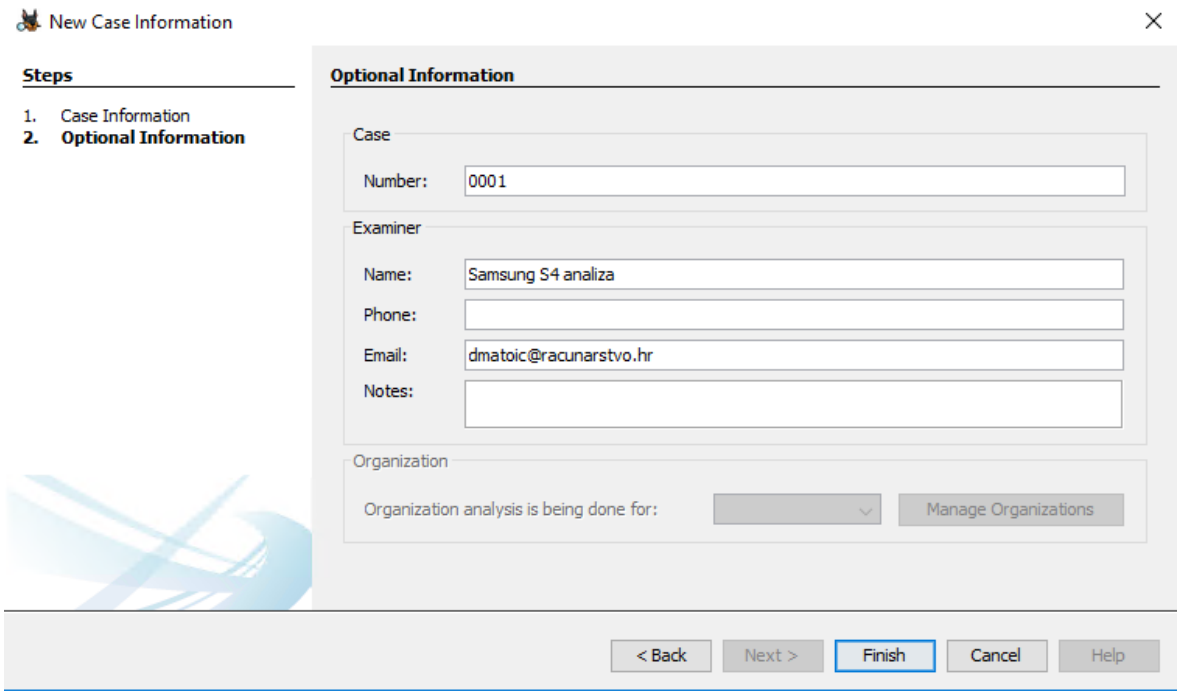
7.2. Analiza slike uređaja alatom Autopsy

Autopsy se može preuzeti sa poveznice http://www.sleuthkit.org/autopsy/ i za potrebe analize preuzet je verzija 64-bit. Nakon instalacije aplikaciju treba pokrenuti i odabirom izbornika Case, odabrati New Case što otvara dijaloški prozor Kreiranje novog slučaja. Nakon što je izvršen upis imena slučaja i putanje baze, klikom na tipku *Next* i prelazi na slijedeći prozor Opcionalne informacije, gdje se nakon njihovog unosa isti potvrdi pritiskom na tipku *Next*

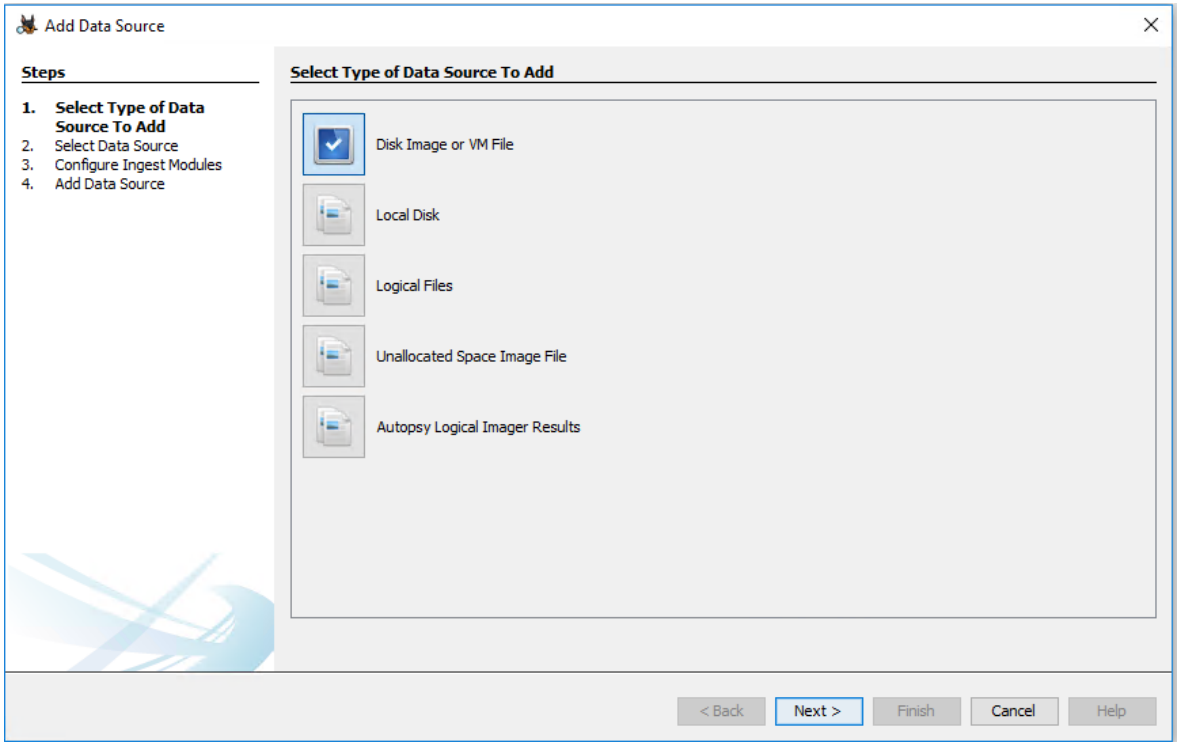


Slika 7.1 Kreiranje novog slučaja[39]

[39] Vlastita slika zaslona računala autora (15.09.2019.)



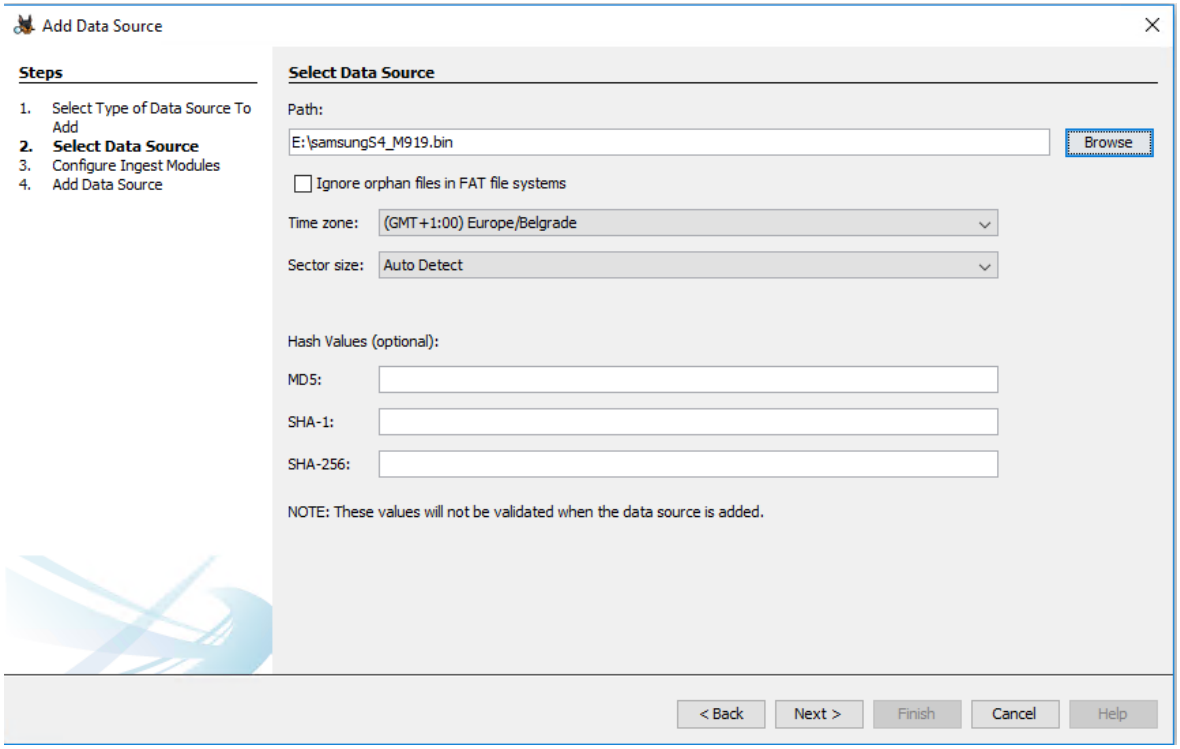
Slika 7.2 Opcionalne informacije[40]



Slika 7.3 Odabir vrste izvora podataka[41]

[40] Vlastita slika zaslona računala autora (15.09.2019.)
[41] Vlastita slika zaslona računala autora (15.09.2019.)

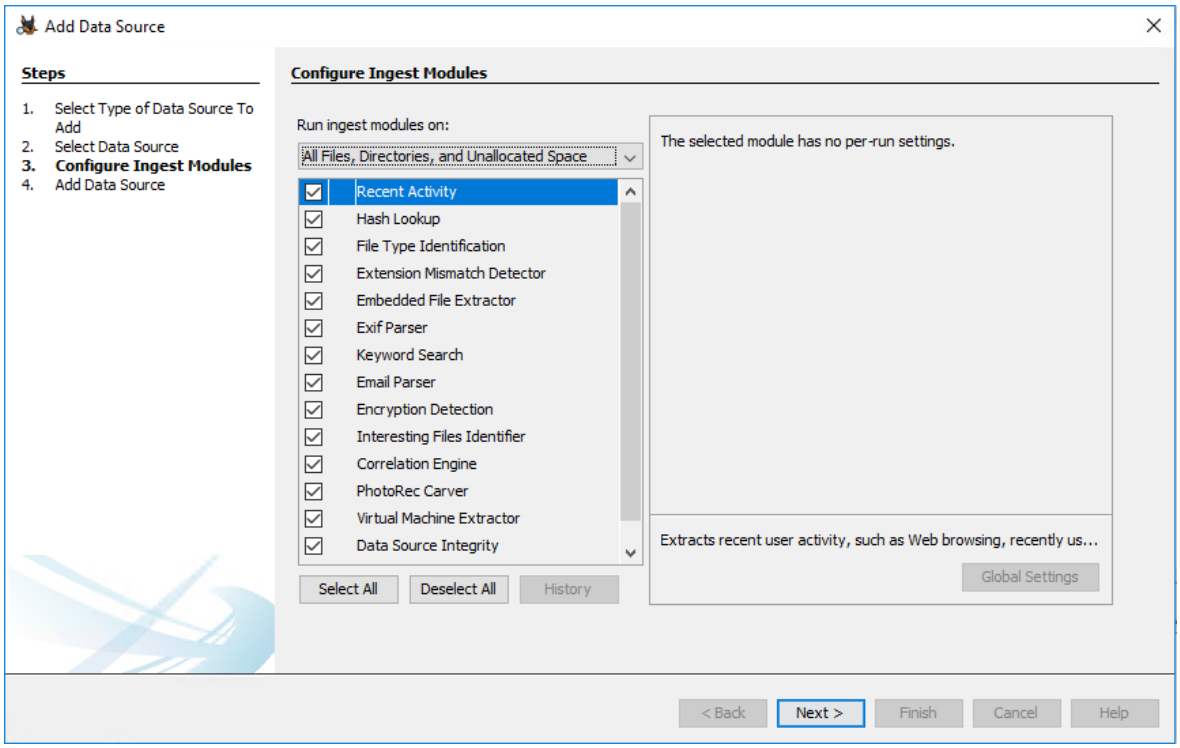
U slijedećem koraku potrebno je izvršiti Odabir vrste izvora podataka i potvrditi pritiskom na tipku *Next*. Pojavit će se prozor Odabir izvora podataka i u ovom dijaloškom okviru potrebno je odabrati putanju do izvorišne datoteke slike memorijske datoteke mobilnog uređaja i potvrditi pritiskom na tipku *Next*.



Slika 7.4 Odabir izvora podataka[42]

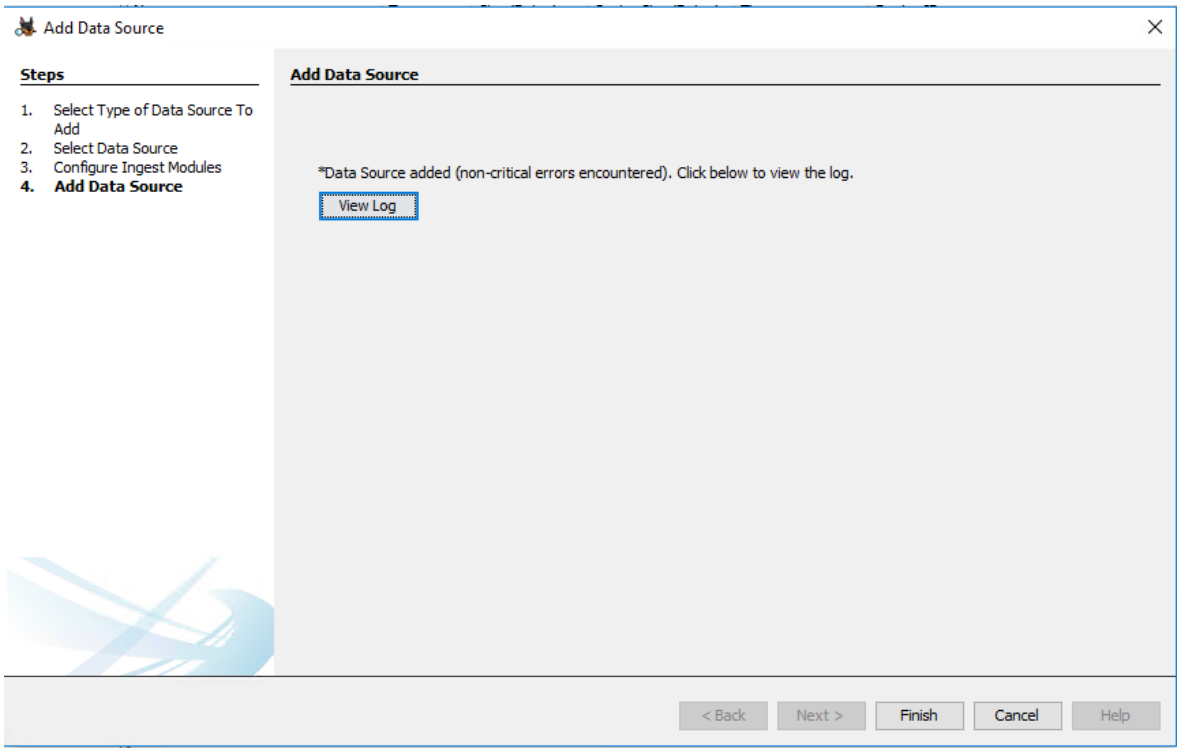
Otvorio se dijaloški okvir za Odabir ispitnih modula. Preporuka je ostaviti sve module uključene, budući da to implicira više rezultata forenzičke analize koja će se pokrenuti sa više načina analize i potrebno je potvrditi odabirom tipke *Next*, što će otvoriti dijaloški okvir za Pogled logova , a po pritisku tipke *Finish*, krenuti će analiza slike sustava, čiji napredak prikazuje Statusna traka.

[42] Vlastita slika zaslona računala autora (15.09.2019.)

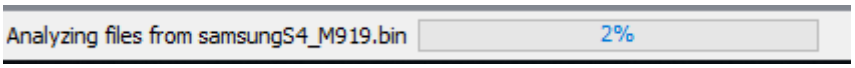


Slika 7.5 Odabir ispitnih modula[43]

[43]Vlastita slika zaslona računala autora (15.09.2019.)



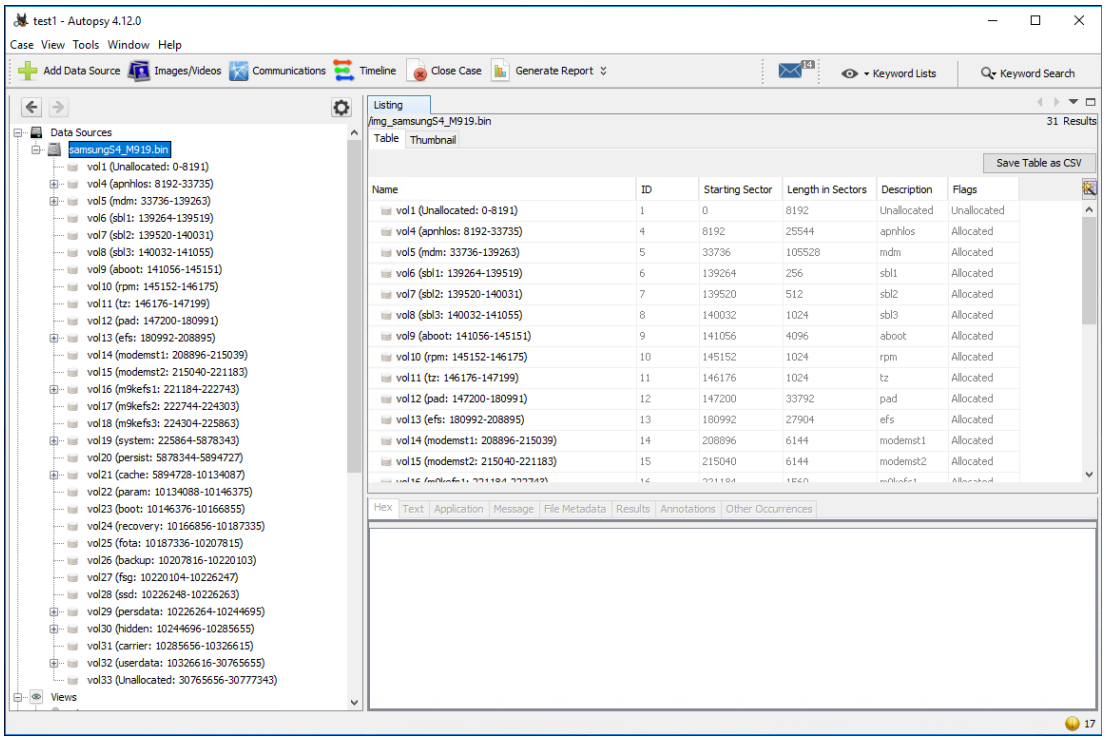
Slika 7.6 Pogled logova[44]



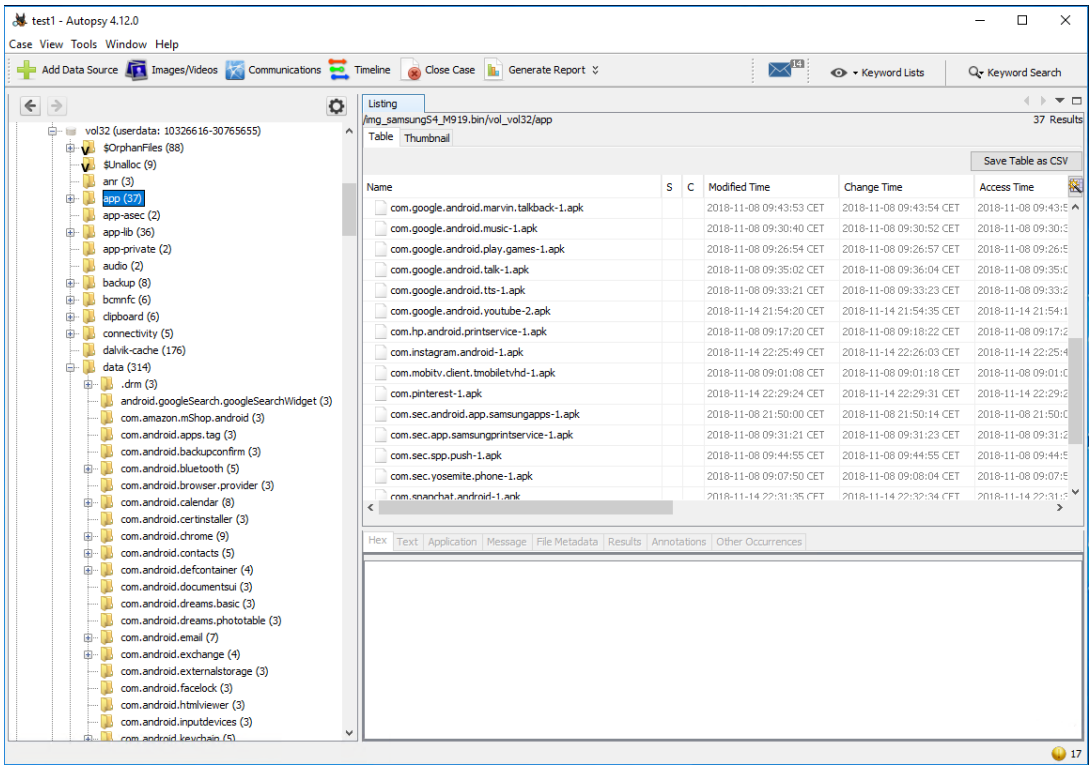
Slika 7.7 Statusna traka[45]

Predmet se počinje učitavati i pokreću se moduli. Analiza slike može početi, a u gornjem lijevom kutu može se proširiti popis particija i volumena koji se nalaze u slici memorije uređaja.

[44] Vlastita slika zaslona računala autora (15.09.2019.)
[45] Vlastita slika zaslona računala autora (15.09.2019.)



Slika 7.8 Izgled sučelja alata Autopsy[46]

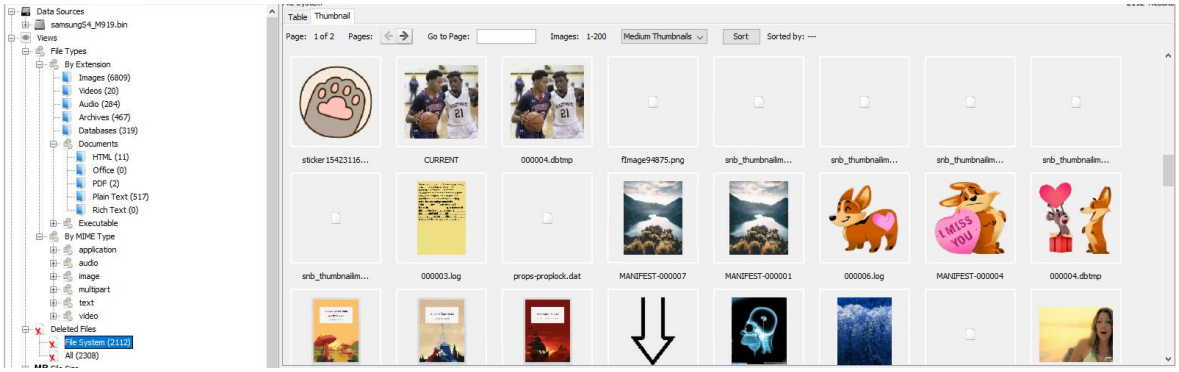


Slika 7.9 Lokacija korisničkih podataka[47]

[46] Vlastita slika zaslona računala autora (15.09.2019.)
[47] Vlastita slika zaslona računala autora (15.09.2019.)

Autopsy otkriva da se na vol32 particiji nalazi Lokacija korisničkih podataka. Na toj particiji postoje mape app, gdje su .apk instalacijske datoteke svih aplikacija instaliranih u mobilnom uređaju, a također i sadržaj mape `/data` gdje se nalaze korisnički podaci aplikacija. Do korisničkih podataka može se doći ako je poznata putanju do podataka pojedine aplikacije ili direktno kroz izbornik View u lijevom prozoru aplikacije, gdje ima puno kriterija za grupiranje pojedinih tipova podataka. Ti kriteriji su grupirane datoteke identificirane modulom identifikacije vrste datoteka.

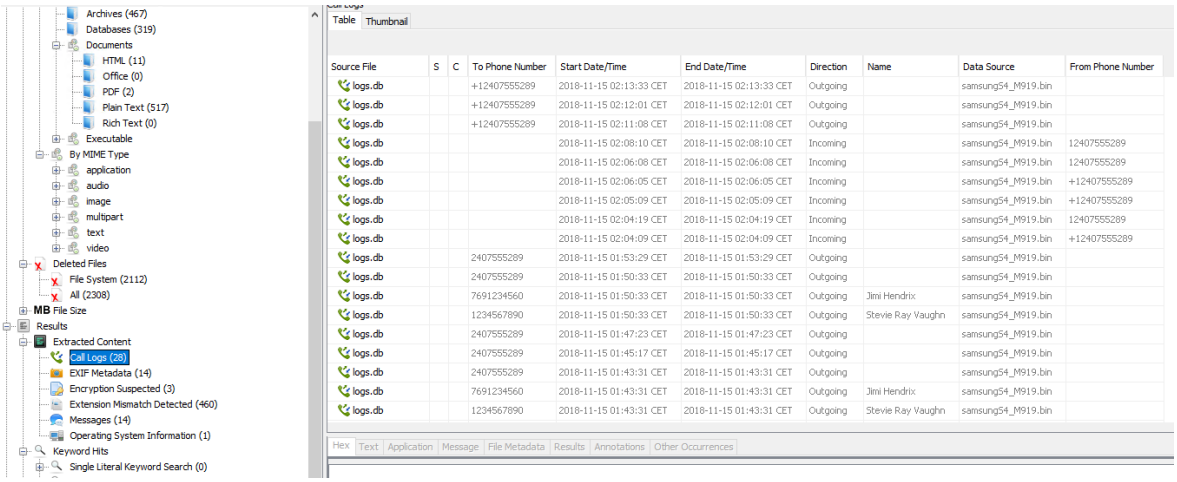
Ovdje postoji pogled Deleted Files, koji se odnosi na datoteke obrisane od strane korisnika, ali kako je u radu prije objašnjeno, podaci su ostali u uređaju i Autopsy ih prikazuje.



Slika 7.10 Deleted Files[48]

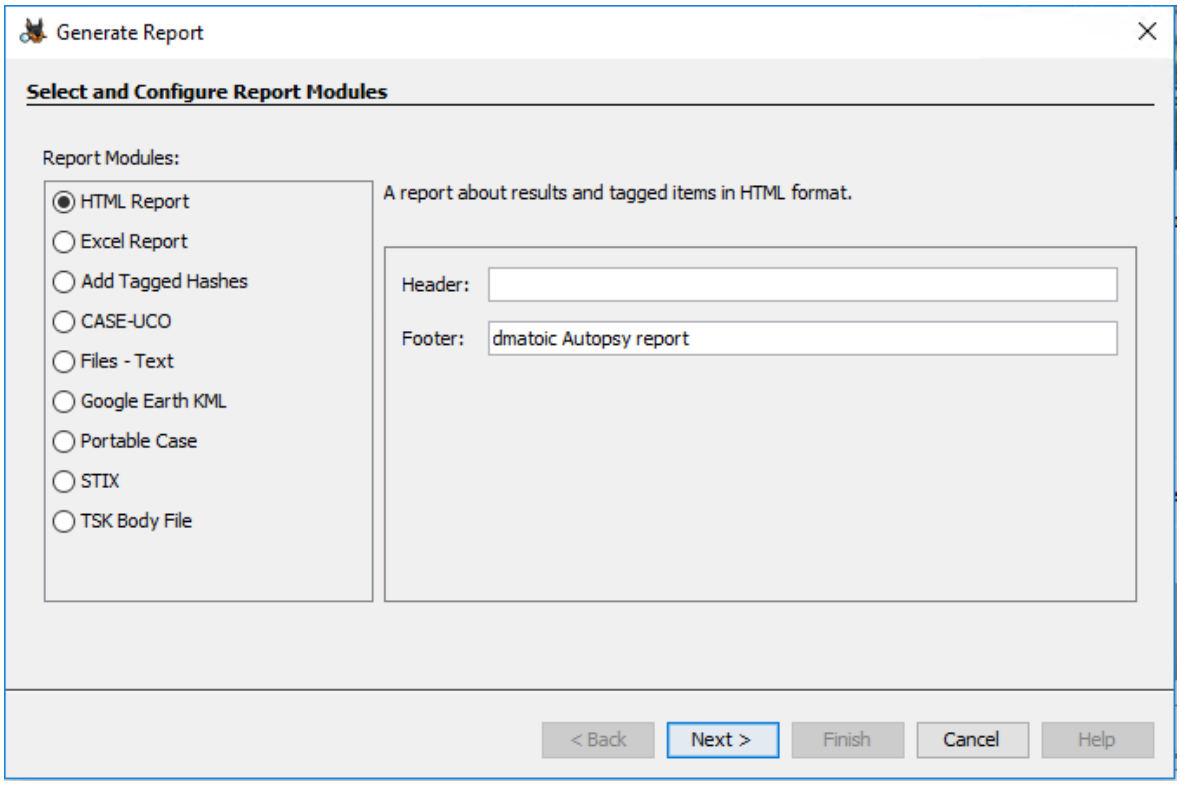
Nadalje, važno je istaknuti Pogled Extracted Content gdje su podaci o komunikaciji odmah dostupni bez da se zna gdje se nalazi pojedina baza s tim podacima. Tako je vidljiv ispis poziva, SMS poruke, EXIF podatke o slikama, itd.

[48]Vlastita slika zaslona računala autora (15.09.2019.)



Slika 7.11 Pogled Extracted Content[49]

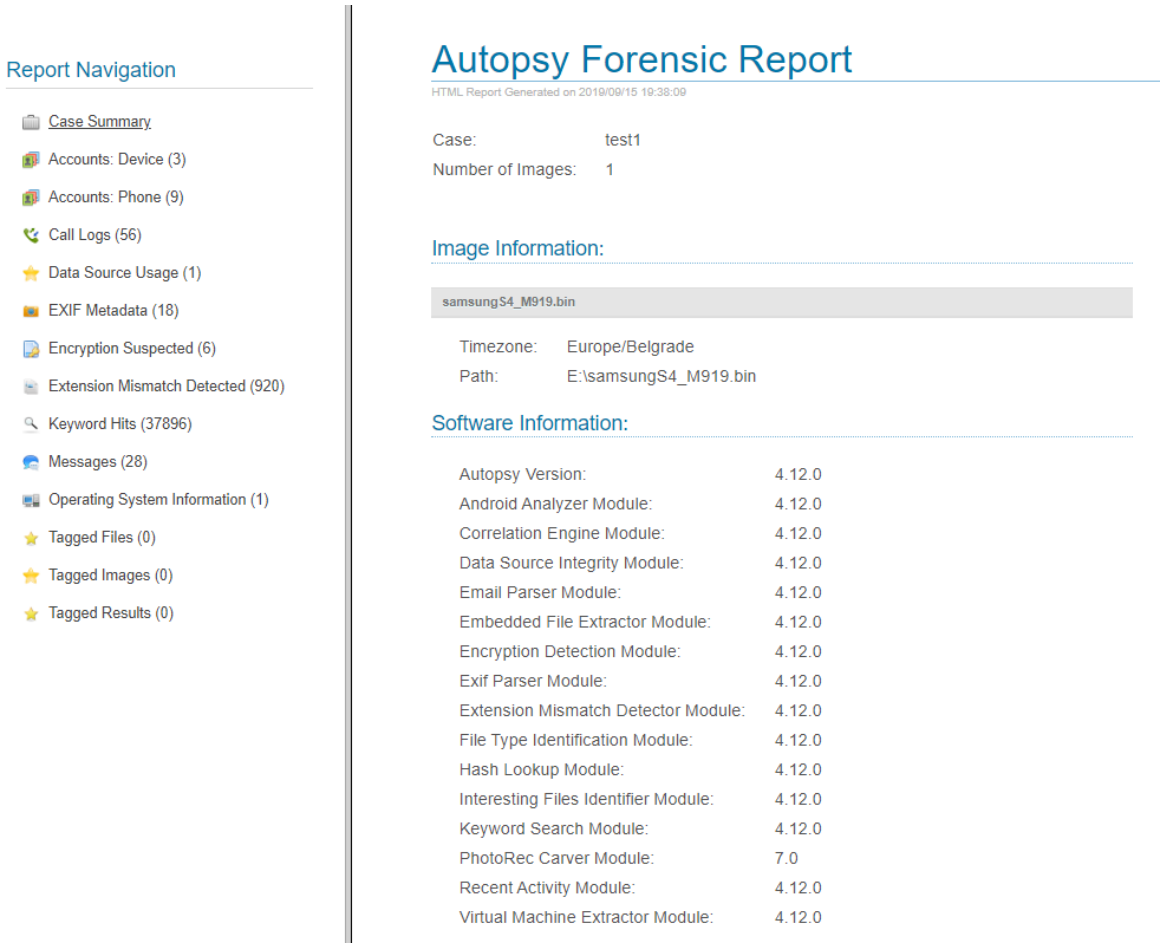
Nakon završene analize forenzičar može kreirati izvješće odabirom Generate Report, otvara se dijaloški prozor u kojem se vrši odabir formata izvještaja



Slika 7.12 Generate Report[50]

Nakon toga potrebno je odabrati još koji će sve rezultati biti u izvještaju. Za potrebe konkretne analize odabran je html izvještaj čiji sadržaj se vidi na slici .

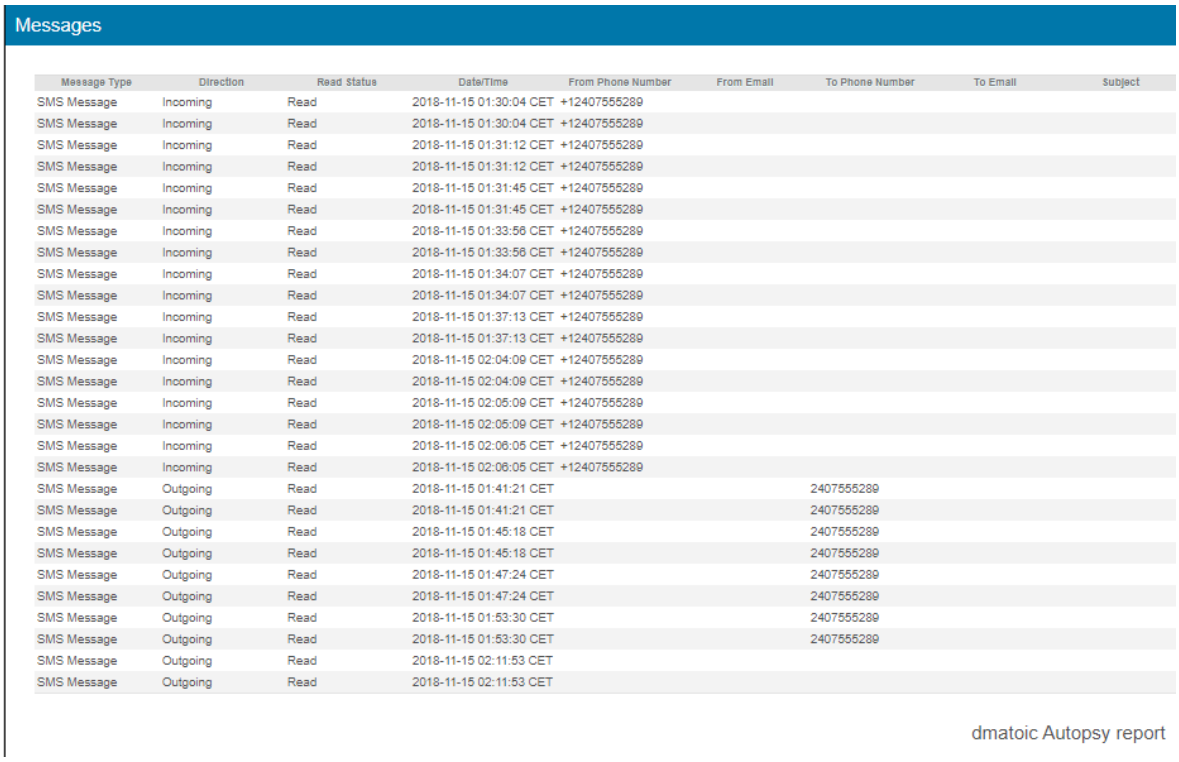
[49] Vlastita slika zaslona računala autora (15.09.2019.)
[50] Vlastita slika zaslona računala autora (15.09.2019.)



Slika 7.13 Početna stranica forenzičkog izvještaja alata Autopsy[51]

Za usporedbu sa službenim izvješćem o analizi slike od strane NIST-a uzete su SMS poruke koje se u izvješću vide na stranici **Error! Bookmark not defined.**, a na dobivenoj analizi vidljive su na slijedećoj slici.

[51] Vlastita slika zaslona računala autora (15.09.2019.)



Messages

Message Type	Direction	Read Status	Date/Time	From Phone Number	From Email	To Phone Number	To Email	Subject
SMS Message	Incoming	Read	2018-11-15 01:30:04 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:30:04 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:31:12 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:31:12 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:31:45 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:31:45 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:33:56 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:33:56 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:34:07 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:34:07 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:37:13 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 01:37:13 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 02:04:09 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 02:04:09 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 02:05:09 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 02:05:09 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 02:06:05 CET	+12407555289				
SMS Message	Incoming	Read	2018-11-15 02:06:05 CET	+12407555289				
SMS Message	Outgoing	Read	2018-11-15 01:41:21 CET			2407555289		
SMS Message	Outgoing	Read	2018-11-15 01:41:21 CET			2407555289		
SMS Message	Outgoing	Read	2018-11-15 01:45:18 CET			2407555289		
SMS Message	Outgoing	Read	2018-11-15 01:45:18 CET			2407555289		
SMS Message	Outgoing	Read	2018-11-15 01:47:24 CET			2407555289		
SMS Message	Outgoing	Read	2018-11-15 01:47:24 CET			2407555289		
SMS Message	Outgoing	Read	2018-11-15 01:53:30 CET			2407555289		
SMS Message	Outgoing	Read	2018-11-15 01:53:30 CET			2407555289		
SMS Message	Outgoing	Read	2018-11-15 02:11:53 CET					
SMS Message	Outgoing	Read	2018-11-15 02:11:53 CET					

Slika 7.14 Prikaz ekstrahiranih SMS poruka[52]

Uz presjek izgleda sučelja i izvještaja aplikacije Autopsy postoji još mnogo funkcionalnosti koje ovdje nisu spomenute, a forenzičarima mogu biti izuzetno korisne. Detaljne upute nalaze se na poveznici http://sleuthkit.org/autopsy/docs/user-docs/4.12.0/ .

[52]Vlastita slika zaslona računala autora (15.09.2019.)

Zaključak

Mobilni uređaji postali su nezaobilazno sredstvo komunikacije u svakodnevnom životu svakog pojedinca. Ta činjenica otvara praktično neograničene mogućnosti ne samo komunikacije, već i svih servisa koji su dostupni putem mobilnih platformi. Uz te dobrobiti mobilne tehnologije, otvara se i mogućnost zloupotrebe, bilo za kriminalne aktivnosti, ali i za kompromitaciju osobnih i poslovnih podataka koji su u mobilnim uređajima pohranjeni.

U radu je obrađena tematika forenzike mobilnih uređaja sa Android operativnim sustavom, budući da je ona najzastupljenija platforma. Definirani su pojmovi računalne forenzike općenito i forenzike mobilnih uređaja. Forenzička analiza mobilnih uređaja zahtjevan je proces koji se mora odvijati po strogo definiranim pravilima kako bi osigurali neporecivost dokaza dobivenih u tom postupku. Mobilna forenzika objašnjena je kroz korake forenzičkog procesa, te karakteristične i važne aktivnosti svakog koraka. Nadalje objašnjena je arhitektura Android operativnog sustava, njegovi sastavni dijelovi i njihova međusobna korelacija. Kroz strukturu particija i datotečnog sustava objašnjen je način pohrane podataka Android mobilnih uređaja kako bi forenzičarima bilo poznato gdje se koji podatak nalazi, kako bi bili što učinkovitiji i trošili čim manje vremena na povrat podataka.

Nakon toga objašnjeni su metode i načini ekstrakcija podataka od logičke i fizičke ekstrakcije do krajnje mjere chip-off postupka i izrade slike memorije mobilnih uređaja. Konceptualno je prezentiran povrat obrisanih podataka iz različitih spremišta.

U pogledu alata za forenzičku analizu spomenuti su lideri područja, EnCase Mobile Investigator, UFED Ultimate i Autopsy, koji je samom činjenicom da je besplatan, ali ima mnoštvo funkcionalnosti i kvalitetan koncept povrata podataka. To je i pokazano na referentnoj preslici interne memorije mobilnog uređaja Samsung Galaxy S4. Pokazan je kompletni postupak od učitavanja slike mobilnog uređaja u aplikaciju do analitike po različitim kriterijima. Pokazano je na koji način se može izvršiti povrat pojedinih tipova podataka.

Rad je dao presjek radnji i postupaka, te načina njihova funkcioniranja za poslove povrata podataka sa mobilnih uređaja sa Android operativnim sustavom.

.

Popis kratica

GPS	Global Positioning System
iOS	Mobile operating system
SDK	Software Development Kit
Root	superuser - special user account
UID	Unique identifier
XML	Extensible Markup Language
ADB	Android Debug Bridge
Wlan	Wireless local area network
Bluetooth	Wireless technology standard for exchanging data
SQLite	Relational database management system
Kernel	Core of a computer's operating system
USB	Universal serial bus
Java API	Java Application programming interface
ART	Android Runtime
DEX	Dalvik Executable
RAM	Random-access memory
daemon	computer program that runs as a background process
UTF	Unicode Transformation Format
micro SD	micro secure digital
FAT32	File Allocation Table
ext3	extended file system version 3
ext4	extended file system version 4
MP	mount point
VFS	Virtual File System
JFS	Journal File System
exFAT	Extended File Allocation Table
F2FS	Flash Friendly File System
JFFS2	Journal Flash File System, verzija 2
LogFS	log-structured and scalable flash file system
UBIFS	flash file system for unmanaged flash memory devices
YAFFS	Yet Another Flash File System
YAFFS2	Yet Another Flash File System version 2

RFS Robust file system

GUI Graphic user interface

OCR Optical Character Recognition

bootloader program that loads an operating system

NIST National Institute of Standards and Technology

CFReDS Computer Forensic Reference Data Sets

Popis slika

Slika 2.1 Relativan broj uređaja po verzijama Android platforme 3
Slika 2.2 Proces forenzike mobilnih uređaja 7
Slika 3.1 Arhitektura android platforme 11
Slika 3.2 Hijerarhija Andoid datoteka 15
Slika 4.1 Uključenje opcije USB Debugging (Način programera) 26
Slika 4.2 Uključenje opcije USB otklanjanje grešaka 30
Slika 4.3 Prikaz popisa mogućih servisa 32
Slika 4.4 Priključeni uređaj na aplikaciju Magnet Acquire 37
Slika 4.5 Odabir vrste ekstrakcije 38
Slika 4.6 Završetak izrade slike mobilnog uređaja 39
Slika 4.7 JTAG programator 40
Slika 4.8 JTAG sučelje mobilnog uređaja 40
Slika 4.9 Mobilni uređaj priključen na JTAG programator 41
Slika 4.10 JTAG aplikacija 41
Slika 4.11 Dataman 48Pro2 Super Fast Universal ISP Programmer 43
Slika 5.1 SQLite Deleted Record Recovery 47
Slika 6.1 EnCase Mobile Investigator 51
Slika 6.2 UFED Ultimate 53
Slika 7.1 Kreiranje novog slučaja 56
Slika 7.2 Opcionalne informacije 57
Slika 7.3 Odabir vrste izvora podataka 57
Slika 7.4 Odabir izvora podataka 58
Slika 7.5 Odabir ispitnih modula 59
Slika 7.6 Pogled logova 60

Slika 7.7 Statusna traka 60
Slika 7.8 Izgled sučelja alata Autopsy 61
Slika 7.9 Lokacija korisničkih podataka 61
Slika 7.10 Deleted Files 62
Slika 7.11 Pogled Extracted Content 63
Slika 7.12 Generate Report 63
Slika 7.13 Početna stranica forenzičkog izvještaja alata Autopsy 64
Slika 7.14 Prikaz ekstrahiranih SMS poruka 65

Literatura

[1] ROHIT TAMMA, OLEG SKULKIN, HEATHER MAHALIK, SATISH BOMMISETTY; *Practical Mobile Forensics;* Third Edition; Packt; January 2018

[2] OLEG SKULKIN, DONNIE TINDALL, ROHIT TAMMA; *Learning Android Forensics Second Edition*; Packt; December 2018

[3] IGOR MIKHAYLOV; *Mobile Forensics Cookbook*; Packt; December 2017

[4] ROHIT TAMMA, DONNIE TINDALL; *Learning Android Forensics*; Packt; April 2015

[5] https://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics (30.3.2019.)

[6] https://developer.android.com/about/dashboards (05.07.2019.)

[7] https://developer.android.com/guide/platform (14.07.2019.)

[8] https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/ (10.7.2019.)

[9] https://dfir.science/2017/04/Imaging-Android-with-root-netcat-and-dd.html (30.08.2019.)

[10] https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective (15.09.2019)

[11] https://resources.infosecinstitute.com/practical-android-phone-forensics/#gref (30.08.2019)

[12] https://www.magnetforensics.com/resources/image-smartphone-magnet-acquire/ (17.08.2019).

[13] https://forensicswiki.org/wiki/JTAG_Samsung_Galaxy_S4_(SGH-I337) (30.08.2019.)

[14] https://www.dataman.com/programmers/universal/dataman-48pro2-super-fast-universal-isp-programmer.html (01.09.2019)

[15] https://accessdata.com/product-download/ftk-imager-version-3-2-0 (10.09.2019.)

[16] https://belkasoft.com/ec (10.09.2019.)

[17] https://www.cellebrite.com/en/ufed-ultimate/ (10.09.2019)

[18] https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective (10.09.2019.)

[19] https://github.com/mdegrazia/SQLite-Deleted-Records-Parser/blob/master/sqlparse_GUI_1_3.zip (11.09.2019.)

[20] http://extundelete.sourceforge.net/ (10.08.2019.)

[21] https://digital-forensics.sans.org/community/downloads (18.06.2019.)

[22] https://www.sans.org/reading-room/whitepapers/analyst/membership/38490 (10.09.2019.)

[23] https://www.guidancesoftware.com/blog/digital-forensics/2017/07/05/three-things-you-need-to-know-about-encase-mobile-investigator (28.08.2019.)

[24] https://cf-media.cellebrite.com/wp-content/uploads/2017/05/DataSheet_UFEDUltimate_A4_2019_web.pdf (28.08.2019.)

[25] https://www.cellebrite.com/en/ufed-ultimate/ (01.09.2019.)

[26] https://www.sleuthkit.org/autopsy/ (01.09.2019.)

[27] https://www.sleuthkit.org/(01.09.2019.)

[28] https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology (22.05.2019.)

Prilog 1 – Primjer izvještaja sadržaja interne memorije mobilnog uređaja Samsung Galaxy S4 – SGH-M919

Appendix A – contains an example/template of a dataset used for populating the internal memory of a mobile device. The format contains data element categories and sub-categories within each root data element.

Samsung Galaxy S4 – SGH-M919

Phone Number: ____

IMEI: 356420053614244

Handset Internal Memory:

<Address Book>

<Long Name (50 chars), Mobile Number>

John Jacob Jingle Heimer Schmidt That's My Name Too

Whenever I Go Out The People Always Shout John Jacob Jingle

Heimer Schmidt

, 8988675309

<Regular Name, Mobile Number, email, website, picture>

Jimi Hendrix, 7691234560, hendrix@experienced.com, website:

www.jimihendrix.com

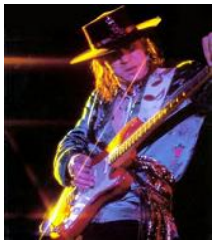
<*Special Character Name, Home Number*>

*, 8887771212

<*Blank Name, Work Number*>

, 8785551111

<*Regular Name, Mobile Number, email, deleted picture, address, birthday*>Stevie Ray Vaughn, 1234567890, work: stevie@srv.com, address: 1234 Main Street, Dallas, TX, SRV Birthday: October 3, 1954,



<*Deleted Entry, Home Number* >

John Bonham, 9878767654

<*Non-ASCII Entry, Mobile Number*>

阿恶哈拉, +86 35 8 763 30 07

<*Non-ASCII Entry, Number*>

Aurélien, +33 22 6 555 20 20

<*Groups contact entry* >

27 Club: Jimi Hendrix*, Stevie Ray Vaughn*, John Bonham

Note: the contact entries within the Group contain data consistent as displayed above.

<PIM Data>

<Datebook/Calendar>

<Long Title (160 chars), Date: 3-03-18, Type: Reminder>

Van halen were scheduled to perform forty shows on their 2007 tour with david lee roth after much success in the early 80s with david lee roth as their front man for van halen!!

<Regular Title, Date: 4-23-18, 6am, Location: Los Angeles Type: Meeting>

Rush concert

NOTE: Viper Room

<Deleted Entryz, Date: 9-16-18, Type: Memo>

Hendrix summer of love documentary

<Entry without Title, Date: 10-10-18, Type: Reminder>

<Special Char Entry, Date: 12-21-18, Type: Reminder>

!

<Memo>

<Long Memo (3000 chars)>

The goal of the CFTT project at NIST is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools capabilities. NIJ has published test reports on several forensic imaging tools, several software write block tools and a variety of hardware write block devices. Currently specifications and test methodologies for deleted file recovery and string searching tools are in development. In addition to forensic tools for acquisition and analysis of digital data on desktop and laptop computers, CFTT is also developing test methodologies for mobile devices. Data acquisition performed on cellular devices operating over Global System for Mobile Communications and non-GSM networks has proven not only frustrating but extremely tedious due to the rapid rate of new cellular devices available on the market. Software vendors specializing in cellular forensics are forced to continuously provide updates to software and associated hardware in order to maintain support and provide examiners with solutions for the latest technologies. Mobile device forensic research performed at the NIST ITL has produced numerous reports on tools capable of acquiring data from Personal Digital Assistants, smart phones, and cellular devices operating over GSM and non-GSM networks. NIST has presented to numerous conferences world-wide providing software vendors, forensic specialists, incident response team members, and law enforcement an overview of the current capabilities and limitations of forensic applications capable of acquiring data from cellular devices as well as suggestions on preservation and handling of digital data. Research conducted over the past two years has produced the following publications: NISTIR 7250 Cell Phone Forensic Tools: An Overview and Analysis, SP800-101 Guidelines on Cell Phone Forensics, NISTIR 7387 Cell Phone Forensic Tools: An Overview and Analysis Update, Forensic Software Tools for Cell Phone Subscriber Identity Modules. In addition to the NIST reports and conference articles produced our research has provided extensive involvement with software engineers from various manufacturers troubleshooting potential issues, providing suggestions on product improvement and overall dependability, which have played a key role in the evolution of cellular forensics software. Research conducted and shared materials have shown to be invaluable insofar as

providing academia with a starting point for education materials, informing law enforcement and forensic examiners of expectations of the interaction between numerous devices and tools, and informing vendors of anomalies while providing a baseline for software improvement.

<*Short Memo*>

This is a short active memo entry.

<*Deleted Memo*>

This entry has been deleted from the memo application.

<Call Logs>

<Missed Calls, non-deleted>

3019753149

<Missed Calls, deleted>

2407555289

<*Incoming, non-deleted*>

3019753149

<*Incoming, deleted*>

3019758140

<*Incoming, deleted*>

9392085319

<*Outgoing, non-deleted*>

3019753149

<Outgoing, deleted>

2407555289

<Incoming SMS Messages, 2407555289>

NOTE: ALL MESSAGES WERE READ!!!

<Message, status: read>

The following SMS message is a read incoming message sent from another device

<Message, status: unread>

The following SMS message is an unread incoming message sent from another device

<Deleted message>

This is a deleted incoming message sent from another device

<Message, status: read, 160 chars>

Incoming read active extended SMS message. This is an incoming SMS message that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message.

<Message, status: unread, 160 chars>

Incoming unread active extended SMS message. This is an incoming SMS message that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message.

<Deleted message>

Incoming deleted extended SMS message. This is a deleted incoming SMS message sent from another device to determine if the forensic application has the ability to acquire and report deleted incoming SMS messages.

<Outgoing SMS Messages[53], 2407555289>

<Message, status: active >

The following SMS message is an active outgoing message sent to another device

<Message, group , 2407555289, Jimi Hendrix, Steve Ray>

The following SMS message is an active outgoing group message sent to multiple recipients

<Deleted message, 2407555289>

This is a deleted outgoing message sent to another device

<Message, status: active, 160 chars, 2407555289>

Outgoing active extended SMS message. This is an outgoing SMS message that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message.

<Message, group 160 chars, 2407555289, Jimi Hendrix, Stevie Vaugh>

Outgoing active extended SMS message. This is an outgoing SMS message sent to multiple recipients that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message.

<Deleted message, 2407555289>

Outgoing deleted extended SMS message. This is a deleted outgoing SMS message sent to another device to determine if the forensic application has the ability to acquire and report deleted outgoing SMS messages.

<Incoming MMS Messages, 2407555289>

[53] Dolazne SMS poruke

<*Message, Audio, read*>

Incoming sound byte MMS message contains the following,

Audio: *Today's Date is: Day, Date, Year*

<*Message, Image, unread*>

Incoming image mms message contains a picture of today's date, Image: *date*

<*Message, Video, read*>

Incoming video message

<Outgoing MMS Messages, 2407555289>

<*Message, Audio, read*>

Outgoing sound byte MMS message contains the following,

Audio: *Today's Date is: Day, Date, Year*

<*Message, Image, unread*>

Outgoing image mms message contains a picture of today's date, Image: *date*

<*Message, Video, read*>

NOTE: couldn't attach the video to the msg, only the text was sent.

Outgoing video message

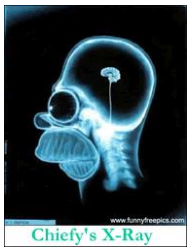
<Stand-alone Data Files>

<*audio*>

mp3 file uploaded to the mobile device

<Active *Images*>

emma-girl.jpg



homer.gif

<*deleted image*>

winter.bmp

<Documents>

<pdf file> forensics.pdf

Forensics is an emerging technology that is branching off into many different avenues (e.g., PDA Forensics, Cell Phone Forensics, Network Forensics, and Stand Alone machine Forensics.

<*video*>

mp4 video file uploaded to the mobile device

<*deleted video*>

mp4 video file uploaded to the mobile device

<Internet Data>

<*Visited Sites*>

www.mobileforensicsworld.org

<*Bookmarked Sites*>

www.phonescoop .com (deleted)

<*Additional Sites* >

www.gmail.com

www.facebook.com

www.twitter.com

www.linkedin.com

login: account1@email.com, account2@email.com

<Email Data>

From: account1

Subject: Photos

Body: The following email contains graphic files. (three attachments)

From: account1

Subject: long memo

Body: The goal of the CFTT project at NIST is...

From: account1

Subject: video

Attachment: video.mp4

From: account1

Subject: audio file

Attachment: audio.wav

From: account1

Subject: audio file

Attachment: audio.mp3

From: account1

Subject: document.pdf

Attachment: document.pdf

From: account1

Subject: document.txt

Attachment: document.txt

<GPS Data >

Current location NIST – Searched for Directions to the Whitehouse

Turn on Geo-tagging and take various pictures and video (document location and which pictures, videos contain geotag information).

- NOTE: Pic and video containing geo-tags are the ones of a laptop.

<**Social Media Data**>

<Facebook>

Account: account1 (John Doe), account2 (Jane Doe)

Profile pic, 3 albums (pics in each), chat logs, wall posts, profile info, video

Account1 – (John Doe)

profile pic:

cover pic:

profile info:

High School: High School 1

College/University: Rhoads University

Employer: TSIN

Current City: House of TTFC

Hometown: City of Angels

Albums: Camaro Pics, Weather Pics, Mobile Uploads

Pics uploaded from phone (Mobile Uploads)-

Chat – account1 to account2: Hello account2, nice pictures account2.

Account1 to account2: This is a deleted Facebook message to determine if tools are able to recover any data remnants.

<Twitter>

Account: account1, account2

Fill out profile information and follow each other, post tweets

Note: account1 and accoutn2 follow each other.

Account1 (tweet): account1 is feeling slightly digital today and needing to tweet a pic.

Personal Message to account2: Hello @account2, thanks for the follow on twitter.

Account2 to account1 (message): Good morning @account1, thank you for the follow back!

<LinkedIn> →**NOTE: device not compatible with the latest version of the app.**

<WhatsApp> → **NOTE: not populated, no SIM card**

<Snapchat>

. Send private messages.

Take some pictures.

<Instagram>

Account: account1, account2

Fill out profile information and follow each other, post pics and videos. Send private messages.

Note: account1 and accoutn2 follow each other

<Pinterest>

Send pictures

Pin something

Diplomski rad može imati priloge, ali se oni ne prilažu uz pisanu verziju diplomskog rada već se mogu priložiti na diplomskom ispitu ukoliko povjerenstvo na diplomskom ispitu tako odluči. Važno je čuvati svu poratnu dokumentaciju koja je nastala pri izradi diplomskog rada.

S unutarnje strane na zadnjim koricama originala, kao i svake kopije diplomskog rada, pričvršćuje se CD s kompletnim diplomskim radom u izvornom formatu (npr. .docx) i .pdf formatu sa svom popratnom dokumentacijom i programima. Pri čemu je obvezno da na tom CD- u postoji i dokument koji opisuje kako se rezultat njegova diplomskog rada (softver ili hardver) koristi (ili kako se npr. izvode mjerenja koja je opisao u radu). Ako se radi o softveru nužno je opisati i kako se programska podrška instalira.