Analiza značajki alata SPF Pro u forenzici mobilnih uređaja

Stepić, Matija

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:142084

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-25**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Matija Stepić

ANALIZA ZNAČAJKI ALATA SPF PRO U FORENZICI MOBILNIH UREĐAJA

DIPLOMSKI RAD

Zagreb, 2019.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

ANALIZA ZNAČAJKI ALATA SPF PRO U FORENZICI MOBILNIH UREĐAJA

ANALYSIS OF SPF PRO TOOL FEATURES IN MOBILE FORENSICS

Mentor: dr. sc. Siniša Husnjak

Student: Matija Stepić
JMBAG: 0135237627

Zagreb, rujan 2019.

ZAHVALA

Zahvaljujem se svom bratiću Antoniju na lektoriranju ovog diplomskog rada te podršci i svim lijepim trenutcima tijekom mog studiranja.

Također, velika zahvala pripada mojoj djevojci Mateji i svim mojim prijateljima koji su uvijek bili uz mene i bez kojih moje studiranje ne bi prošlo tako lako i zabavno.

Posebno se zahvaljujem mentoru dr. sc. Siniši Husnjaku na prenesenom znanju, pomoći, savjetima te uloženom trudu i vremenu pri izradi ovog diplomskog rada.

Najveća zahvala pripada mojoj obitelji koja je uvijek bila tu za mene i pružala mi najveću podršku i razumijevanje i bez koje sve ovo ne bi bilo moguće.

ANALIZA ZNAČAJKI ALATA SPF PRO U FORENZICI MOBILNIH UREĐAJA

SAŽETAK

Digitalna forenzika jedna je od grana forenzičkih znanosti, a osnovna zadaća joj je otkrivanje i tumačenje elektroničkih podataka. Digitalna forenzika sastoji se od mnogo grana, a jedna od njih je mobilna forenzika koja je usmjerena otkrivanju i tumačenju digitalnih dokaza s mobilnih uređaja. Osnovni cilj forenzičkih ispitivanja je očuvanje podataka u izvornom obliku. Forenzička analiza provodi se primjenom brojnih metoda poput ručne, logičke, datotečne i fizičke ekstrakcije. Te metode nalaze se u sklopu određenih forenzičkih alata koje provode forenzički istražitelji. Ekstrakcija podataka je pojam koji se odnosi na dohvaćanje podataka u cilju daljnje obrade i pohrane. Tijekom provođenja forenzičke analize forenzički istražitelji susreću se s brojnim izazovima kao i antiforenzikom koja onemogućava ekstrakciju podataka mobilnih uređaja. Forenzički alati se prema osnovnoj podjeli dijele na softverske i hardverske alate. Oni su namijenjeni za pomoć forenzičkim istražiteljima u prikupljanju, očuvanju i ispitivanju digitalnih dokaza s mobilnih uređaja. Jedan od alata mobilne forenzike je softverski alat SPF Pro kineske tvrtke SalvationDATA. Korištenje alata SPF Pro je vrlo jednostavno, no u usporedbi s ostalim alatima iste namjene predstavlja se kao nedovoljno dobar izbor. Alat je usmjeren kineskim mobilnim uređajima te uređajima koji imaju ostvaren *Root* pristup. Za ostale uređaje alat ne omogućava provođenje velikog broja metoda ekstrakcije.

KLJUČNE RIJEČI: mobilni uređaj; mobilna forenzika; ekstrakcija podataka; forenzički alat; SPF Pro; analiza podataka

SUMMARY

Digital forensics is one of the branches of forensic science and its primary task is to detect and interpret electronic data. Digital forensics consists of many branches and one of them is mobile forensics, which is aimed to detect and interpret digital evidence from mobile devices. The main goal of forensic investigation is preserving data in its original form. Forensic analysis is performed by using a number of methods, such as: manual, logical, file and manual extraction. These methods can be find in forensic tools and task for forensic investigators is to implement them. Data extraction is a term that refers to the retrieval of data for further processing and storage. During forensic analysis, forensic investigators face numerous challenges as well as antiforensics that inhibits the extraction of mobile device data. Forensic tools are divided into software and hardware tools by basic division, and they are intended to assist forensic investigators in collecting, preserving and examining digital evidence from mobile devices. One of the tools of mobile forensics is the software tool SPF Pro from Chinese company SalvationDATA. Using SPF Pro is very simple, but in comparison to other tools of the same purpose, it seems like it is not a proper choice. The tool is targeted at Chinese mobile devices and devices that have *Root* access. For other devices, the tool does not allow a large number of extraction methods to be performed.

KEY WORDS: mobile device; mobile forensics; data extraction; forensic tool; SPF Pro; data analysis

Sadržaj

1. Uvod

Današnje vrijeme, u kojem su digitalne tehnologije značajno napredovale, rezultiralo je velikim brojem mobilnih uređaja na tržištu. Mobilni uređaji postali su sastavni dio života većine ljudi te se svakodnevno koriste u različite svrhe. Većina ljudi koristi mobilne uređaje kao sredstvo za odvijanje komunikacije te za obavljanje svakodnevnih aktivnosti. Kako se mobilni uređaji mogu koristiti za legalne svrhe, tako mogu i za ilegalne kao što je planiranje i počinjenje određenog kaznenog djela. Mobilni uređaji ostavljaju tragove koji mogu otkriti i razriješiti određeni slučaj, a predstavljaju i veliki izvor digitalnih dokaza. Za dobavljanje tih digitalnih dokaza primjenjuje se postupak forenzičke analize mobilnih uređaja. Forenzička analiza mobilnih uređaja predstavlja postupak otkrivanja, oporavka i analize digitalnih dokaza s mobilnih uređaja na način da se digitalni dokazi ne izmijene. Za provođenje forenzičke analize zaduženi su forenzički istražitelji koji putem raznih forenzičkih alata pokušavaju doći do korisnih podataka. Kako bi forenzički istražitelji na uspješan i prihvatljiv način ekstrahirali podatke mobilnih uređaja moraju biti dobro obučeni.

Ekstrakcija podataka predstavlja pojam koji se odnosi na dohvaćanje podataka iz različitih izvora u cilju daljnje obrade i pohrane. Ona predstavlja najvažniji i najsloženiji dio cijelog postupka forenzičke analize. Način, odnosno metode i faze kojima se provodi opisane su u trećem poglavlju, a za svaku od njih navedene su ključne karakteristike te prednosti i nedostaci. Ekstrakcija se izvodi metodama koje su dostupne u sklopu određenog forenzičkog alata koji mogu biti hardverski ili softverski.

Osnovni predmet promatranja ovog diplomskog rada je softverski forenzički alat SPF Pro tvrtke SalvationDATA. Četvrto, peto i šesto poglavlje daju uvid u način rada alata, kao i njegove osnovne značajke tijekom procesa ekstrakcije podataka s četiri različita mobilna uređaja (Samsung Galaxy S3 Mini, Samsung Galaxy A5, HTC Desire 610 te iPhone 4). Cilj svakog forenzičkog ispitivanja je pronaći i ekstrahirati digitalne dokaze koji mogu biti korisni za rješavanje određenog slučaja. Postupak ekstrakcije podataka proveden je za sve navedene uređaje, a količina ekstrahiranih podataka pojedinog uređaja vidljiva je u šestom poglavlju.

Cilj i svrha ovog diplomskog rada je analizirati mogućnosti alata SPF Pro u forenzici mobilnih uređaja te objasniti njegov način rada.

Diplomski rad sastoji se od 7 poglavlja:

1. Uvod
2. Forenzička analiza mobilnih terminalnih uređaja
3. Sistematizacija metoda i postupaka ekstrakcije podataka
4. Karakteristike forenzičkog alata SPF Pro
5. Provedba forenzičke analize korištenjem alata SPF Pro
6. Validacija i analiza ekstrahiranih podataka
7. Zaključak

U drugom poglavlju definiraju se osnovni pojmovi digitalnog dokaza, digitalne i mobilne forenzike, navode se izazovi s kojima se forenzički istražitelji susreću, kao i zlonamjerne metode koje otežavaju postupak forenzičke analize, a nazivaju se antiforenzičke metode.

Trećim poglavljem opisuju se osnovne značajke ekstrakcije podataka, faze kojima se ekstrakcija provodi te razne metode putem kojih se ekstrakcija izvršava.

Četvrto poglavlje opisuje glavne značajke forenzičkog alata SPF Pro. Prikazuju se njegove ključne značajke te način na koji on radi, a opisuju se i brojni dodatni alati koji olakšavaju izvođenje ekstrakcije podataka. Također, uspoređuje se forenzički alat SPF Pro prema njegovim mogućnostima u odnosu na druge alate iste namjene.

U petom poglavlju prikazuje se način na koji se izvršava ekstrakcija podataka za pojedini mobilni uređaj. Prikazuju se metode te načini njihove provedbe za pojedine mobilne uređaje.

Šesto poglavlje obuhvaća analizu i validaciju svih ekstrahiranih podataka za pojedine mobilne uređaje. Opisuju se načini analize podataka unutar alata SPF Pro te se uspoređuju ekstrahirani podaci mobilnih uređaja. Uz to, SPF Pro se uspoređuje s drugim alatima iste namjene prema količini ekstrahiranih podataka.

2. Forenzička analiza mobilnih terminalnih uređaja

Pojam forenzike predstavlja naziv za primjenu širokog spektra znanstvenih grana za utvrđivanje činjenica u različitim sudskim ili drugim postupcima. Napretkom moderne tehnologije u današnje vrijeme sve se češće spominje pojam forenzičke analize. Forenzika se sastoji od velikog broja grana. Prva pomisao ljudi na pojam forenzike su razni kriminalistički filmovi koji se bave istraživanjem zločina na licu mjesta. Postoji mnogo definicija i tumačenja forenzike. Jedna od njih je da je forenzika otkrivanje tragova ili dokaza koristeći razne alate, metodologije i procese te primjena znanstvenih grana za utvrđivanje činjenica. Ovaj diplomski rad temeljen je na mobilnoj forenzici koja je dio digitalne forenzike. Glavno pravilo forenzike, odnosno provođenja forenzičke analize je očuvanje dokaza u izvornom obliku kako bi se mogli koristiti u sudskim postupcima, [1].

2.1. Digitalna forenzika

Digitalna forenzika dio je forenzičkih znanosti, a ona predstavlja proces otkrivanja i tumačenja elektroničkih podataka, [2]. Može se reći da je digitalna forenzika primjena znanstvenih načela u procesu otkrivanja informacija s digitalnog uređaja. Prvi oblik digitalne forenzike bio je pokrenut gotovo u isto vrijeme kada su upotrebljena i računala, no sposobnosti digitalne forenzike od tada su značajno napredovale, a taj napredak se očituje i danas. Digitalna forenzika može uključivati gotovo sve digitalne uređaje, a ne samo računala. Neka od uobičajenih područja u kojima se digitalna forenzika primjenjuje uključuju računala, pisače, mobilne uređaje, fiksne telefone, globalne sustave pozicioniranja (GPS, engl. *Global Positioning System*) i medije za pohranu. Manje razvijena područja uključuju uredsku opremu i druge programabilne uređaje dok je trenutno u razvoju forenzika automobila odnosno njihovih sustava, [3].

Cilj svakog forenzičkog ispitivanja pa tako i digitalnog forenzičkog ispitivanja je čuvanje dokaza u originalnom obliku koje uključuje prikupljanje, identificiranje i provjeru digitalnih informacija, odnosno digitalnih dokaza u svrhu rekonstrukcije prethodnih događaja. Pojam digitalne forenzičke analize najčešće se stavlja u kontekst prikazivanja digitalnih podataka na sudu kako bi se rekonstruirao pojedini događaj. Osim toga, digitalna forenzička analiza ima znatno veći utjecaj na cjelokupno društvo i sigurnost gdje se mogu spriječiti određena zlonamjerna djela, nasilje na Internetu te mnogobrojne druge aktivnosti, [2]. Također, može se koristiti za rješavanje problema u korporacijskom okruženju, kao npr. oporavak izgubljenih datoteka ili rekonstruiranje informacija iz oštećene opreme te za ispitivanje promjena na uređajima koji podliježu stimulaciji, [3].

Jedan od najuobičajenijih digitalnih uređaja u današnjem vremenu je mobilni uređaj. Činjenica je da su se mobilni uređaji probili u svakodnevni život i da se koriste za mnogo više aktivnosti, nego je to bilo u prošlim vremenima, kada su se oni isključivo upotrebljavali za

pozive, odnosno poruke. Moderni mobilni uređaji poistovjećuju se s računalima pa ih njihovi vlasnici ne koriste isključivo samo za komunikaciju nego i za pohranu, organizaciju i obradu podataka, za pregledavanje Interneta, fotografiranje, i sl. Ovaj rad usmjeren je na mobilne uređaje i mobilnu forenziku koja će biti detaljno objašnjena u nastavku, [4].

2.1.1. Primjena digitalne forenzike

Forenzička analiza digitalnih dokaza može imati značajnu ulogu u širokom rasponu slučajeva, a u nekim slučajevima može biti ključna u vođenju forenzičkog istražitelja do počinitelja kaznenog djela. Digitalna forenzika primjenjuje se za sljedeće aktivnosti:

- **Uspostavljanje veza** – Prvi je način primjene digitalne forenzike. Digitalna forenzička analiza može imati izravnu ulogu u identificiranju i uhićenju počinitelja, pomažući istražiteljima u uspostavljanju veza između ljudi i njihovih aktivnosti na Internetu. Međutim, pripisivanje aktivnosti na uređaju ili Internetu određenom pojedincu može biti veliki izazov. Na primjer, zapisi koji pokazuju da je određeni račun na Internetu korišten za počinjenje kaznenog djela ne dokazuju da je vlasnik tog računa bio odgovoran za kazneno djelo, jer je taj račun mogao koristiti i netko drugi, [4]. Korištenje dokaza iz više neovisnih izvora za međusobno potkrepljivanje i razvijanje točne slike događaja može pomoći razviti snažnu povezanost između pojedinca i aktivnosti na uređaju, [5].
- **Razmatranje alibija i izjava** - Prijestupnici i žrtve mogu namjerno ili nesvjesno zavarati istražitelje tvrdeći da se nešto dogodilo ili da su bili negdje u određeno vrijeme. Pomoću unakrsne usporedbe takvih informacija s digitalnim tragovima koje ostavljaju aktivnosti neke osobe, može se naći digitalni dokaz koji podržava ili opovrgava izjavu ili alibi. Istražitelji se ne bi trebali oslanjati na jedan dio digitalnog dokaza kada ispituju alibi, već bi trebali pokušavati pronaći povezani lanac digitalnih dokaza. Također, istražitelji moraju uzeti u obzir da razmatranje alibija predstavlja veliki izazov jer je teško dokazati tko je koristio mobilni uređaj u određeno vrijeme, osobito kada se mobilni uređaji ili SIM kartice dijele među članovima grupe ili obitelji, [4]. Postoji mogućnost da ljudi koji su predmet istrage, programiraju odnosno zakažu određenu radnju, kao što je slanje poruke e-pošte, kako bi zavarali istražitelje i na neki način opravdali svoj alibi, [5].
- **Određivanje namjere** - Odnosi se na utvrđivanje ponašanja i misli određenog korisnika mobilnog uređaja. Analiza uređaja kojeg pojedinac koristi može otkriti njegove najdublje misli u određenom trenutku. Na mobilnom uređaju moguće je naći jasne dokaze o namjeri počinjenja određenog djela poput dnevnika ili zapisa aktivnosti na uređaju. Forenzička analiza digitalnih uređaja može otkriti druga ponašanja koja mogu biti vrlo korisna za određivanje namjere, [4].
- **Ocjena izvora** - Forenzički istražitelji obično su traženi da daju uvid u podrijetlo određene stavke digitalnog dokaza. Osim određivanja porijekla poruke e-pošte koristeći IP adrese, različiti formati datoteka imaju karakteristike koje mogu biti

povezane s njihovim izvorom. Ako uređaj osumnjičenog sadrži fotografije koje se odnose na neki zločin, nije moguće s velikom sigurnosti pretpostaviti da je osumnjičeni i stvorio te fotografije. Moguće je da su datoteke kopirane iz drugog sustava ili preuzete s Interneta. Važan dio forenzičke istrage su metapodaci koji se pohranjuju za svaku preuzetu ili stvorenu fotografiju, što se može upotrijebiti za dokazivanje izvora fotografije. [5].

- **Autentičnost digitalnog dokumenta** - Autor dokumenta i datum izrade mogu biti vrlo značajni za tijek istrage, iako nekad počinitelji kaznenih djela sakrivaju i krivotvore te podatke. Relativno je jednostavno promijeniti te podatke no postoje različiti pristupi koje forenzički istražitelji koriste kako bi se provjerila autentičnost digitalnog dokumenta. Forenzički istražitelji mogu koristiti datoteke datuma i vremena te log zapise kako bi utvrdili porijeklo dokumenta. Na primjer, moguće je otkriti krivotvorenje i dokumentiranje krivotvorenja tragajući za kronološkim nedosljednostima u log datotekama i datotekama za označavanje datuma i vremena, [6].

2.1.2. Digitalni dokaz

Dokazima se smatra sve ono što razdvaja hipotezu od neosnovane tvrdnje, a oni mogu potvrditi ili pobiti hipotezu, stoga je njihov integritet vrlo bitan u prihvaćanju, odnosno poricanju pred sudovima. Postoji mnogo definicija digitalnog dokaza. Jedna od njih koja se često spominje govori da je digitalni dokaz informacija uskladištena ili prenošena u digitalnoj formi koja se može koristiti u sudskim postupcima. Pod pojmom digitalna forma smatraju se elektronski ili magnetni uređaji, pa to mogu biti podaci u memoriji, aplikacijama, ali i podaci koji se nalaze u prijenosu, tj. transmisiji, kao što su radiovalovi, [7].

Dvije su osnovne vrste digitalnih dokaza [8]:

- **Aktivni** – Stvara ih korisnik kroz interakciju sa sustavom (npr. pohrana fotografija)
- **Pasivni** – Kreira ih sustav bez znanja korisnika (log zapisi, bilježenje događaja unutar operativnog sustava)

2.1.2.1. Forma i analiza digitalnog dokaza

Digitalni dokaz nije jednostavan pojam i nije nešto što obični ljudi na prvi pogled mogu protumačiti. Ako bi se digitalni dokaz sagledao u doslovnom smislu, on bi predstavljao niz nula i jedinica koje neki uređaj pretvara u oblik razumljiv ljudima, a koji ga onda mogu tumačiti i koristiti u sudskim postupcima, [9]. Digitalna forenzika usmjerena je određivanju forme digitalnog dokaza, pa su tako digitalni dokazi klasificirani prema skladištenju podataka na:

- **Privremena forma**– Primjer ove forme je RAM memorija kod koje se podaci bez vanjskog izvora napajanja brišu.
- **Nestalna forma** – Kod ove forme karakteristično je da postoji neki unutarnji izvor napajanja kao što je baterija. Kao i kod privremene forme, ako je baterija izvađena, podaci će biti izgubljeni. Primjer nestalne forme je CMOS ili RAM na prijenosnom računalu koje ima napajanje na bateriju.
- **Polustalna forma** – Polustalna forma odnosi se na čvrste medije s mogućnošću promjene. Primjeri polustalne odnosno semipermanentne forme su hard disk, disketa, CD, DVD, memorijske kartice.
- **Stalna forma** – Stalna forma je ROM memorija koja je uvijek postojana i podaci se ne gube nestankom napajanja.

Analiza digitalnih dokaza ovisi o vrsti forenzičke istrage koja se provodi. To mogu biti računalna, mrežna, forenzika elektroničke pošte, mobilnih uređaja. Kako je već prethodno navedeno, potrebno je stvoriti identičnu kopiju digitalnih dokaza na kojima se mogu vršiti analize i brojne druge radnje, a ta identična kopija naziva se forenzičkom slikom. Nakon što je kreirana forenzička slika, istražitelju preostane potencijalno velika količina podataka, od koje jako mali dio može sadržavati informacije važne za istragu. Kako ručna pretraga svakog dokumenta nije praktična i jako dugo traje, preporučuje se sljedeća strategija pregleda podataka, [10]:

- **Postavljanje pitanja i promatranje** – Ako istražitelj nije uključen u istragu od samog početka, potrebno je prikupiti najosnovnije činjenice i elemente slučaja, odrediti što se očekuje od istrage te na što se sumnja. Kada je to moguće, preporučuje se razgovor i ispitivanje osumnjičenih u svrhu smanjenja kriterija pretrage po podacima.
- **Strategija pretrage mora uključivati liste ključnih riječi i traženih pojmova** – Ovisno o slučaju, nekada je za rješavanje određenog kaznenog djela dovoljno pregledati slike, elektroničku poštu ili mrežni promet.
- **Pregled digitalnih dokaza odvija se prema strategiji razvijenoj u prethodnom koraku** – U postupku forenzičke analize nailazi se na nove dokaze pa se tako ključne riječi ili lokacije traženja mogu mijenjati.
- **Formulacija objašnjenja, interpretacija pronađenih dokaza te kreiranje zaključaka** – Forenzički istražitelji moraju moći objasniti što i kako se dogodilo, a što nije te na koje načine su ekstrahirali podatke.
- **Preispitivanje zaključaka i metoda** – Uzimajući u obzir pronađene dokaze, poželjno je preispitati metode i rezultate te moguće propuste.
- **Izvještaj o zaključcima i pronađenim dokazima** – Na kraju analize digitalnih dokaza potrebno je kreirati izvještaj koji sadrži sve poduzete mjere, korake i alate.

Niti jedan alat ne može interpretirati digitalne dokaze ili doći do traga koji povezuje digitalne dokaze s elementima slučaja, a upravo to je glavna zadaća forenzičkog istražitelja. Forenzički alati mogu se koristiti za strukturiranje upita te kategorizaciju rezultata, no krajnji rezultat ovisi o istražitelju. Sudovi često osporavaju pretrage podataka pa se stoga preporučuje detaljno dokumentiranje svakog koraka, protokola, procedure, itd, [9].

2.1.2.2. Pravila i prihvatljivost digitalnih dokaza

Postoji pet općih pravila digitalnih dokaza koja se primjenjuju na digitalnu forenziku i koja se moraju slijediti kako bi dokazi bili valjani. Ignoriranje ovih pravila čini dokaze nedopuštenima, a predmetni slučaj može biti odbačen. Pravila digitalnih dokaza su:

- **Dopustiv** – To je najosnovnije pravilo i mjerilo valjanosti i važnosti dokaza. Dokazi moraju biti sačuvani i prikupljeni tako da se mogu koristiti na sudu. Mnoge pogreške mogu biti učinjene, a u tim slučajevima sudac može odrediti da je dokaz nedopušten. Na primjer, dokazi koji se prikupljaju protuzakonitim metodama obično se smatraju nedopuštenima.
- **Autentični** – Dokazi moraju biti povezani s incidentom na relevantan način kako bi se nešto dokazalo. Sudski vještak mora biti odgovoran za podrijetlo dokaza.
- **Potpuni** – Kada se dokazi prezentiraju, moraju biti jasni i potpuni te odražavati cijelu priču. Nije dovoljno prikupiti dokaze koji pokazuju samo jednu perspektivu incidenta. Iznošenje nepotpunih dokaza opasnije je ako se uopće ne pruže dokazi, jer to bi moglo dovesti do drugačije presude.
- **Pouzdani** – Dokazi prikupljeni na uređaju moraju biti pouzdani. To ovisi o korištenim alatima i metodologiji. Primijenjene tehnike i prikupljeni dokazi ne smiju dovoditi u pitanje autentičnost dokaza. Ako je ispitivač upotrijebio neke tehnike koje se ne mogu reproducirati, to se ne razmatra osim ako im je to naloženo. To bi uključivalo moguće destruktivne metode kao što je vađenje čipova.
- **Vjerojatni** – Sudski vještak mora biti u stanju jasno i sažeto objasniti koje su procese koristili i na koji način je očuvan integritet dokaza. Dokazi koje je proveo ispitivač moraju biti jasni, lako razumljivi i uvjerljivi, [10].

U većini pravnih sustava i organizacija digitalni dokazi se vrednuju prema tri osnovna načela, a to su: relevantnost, pouzdanost i dosljednost. Ta tri principa važna su za prihvatljivost digitalnih dokaza na sudu.

- Digitalni dokazi relevantni su onda kada se odnose na dokazivanje ili opovrgavanje elemenata konkretnog slučaja.
- Značenje pouzdanosti razlikuje se u ovisnosti o pravnim sustavima, no opće načelo je osiguravanje da su digitalni dokazi ono za što se tvrdi da jesu, te da nisu oštećeni.
- U nekim slučajevima nije uvijek potrebno prikupiti sve podatke ili napraviti kompletnu kopiju originalnog dokaza. U većini pravnih sustava, koncept dosljednosti znači da se dovoljno dokaza treba prikupiti za dokazivanje ili opovrgavanje elementa spornog slučaja, [11].

2.2. Mobilna forenzika

Kao što je navedeno digitalna forenzika je grana forenzičkih znanosti koja je usmjerena na otkrivanje i tumačenje digitalnih podataka koji se nalaze u elektroničkim ili digitalnim uređajima. Jedna od grana digitalne forenzike je mobilna forenzika na koju se stavlja naglasak u ovome radu. Ona se odnosi na otkrivanje, oporavak i tumačenje digitalnih dokaza s mobilnih uređaja. Glavno načelo bilo kojeg forenzičkog ispitivanja je da se izvorni dokazi ne smiju mijenjati jer to može ugroziti njihovu vjerodostojnost. To je pogotovo predstavlja veliki izazov kada se forenzičko ispitivanje provodi nad mobilnim uređajima. Primjer takve poteškoće je da neki forenzički alati zahtijevaju komunikacijski vektor odnosno vezu s mobilnim uređajem tako da standardna zaštita od pisanja neće raditi tijekom forenzičke analize. Druge forenzičke metode prikupljanja podataka s uređaja mogu uključivati uklanjanje čipa ili instaliranje *bootloader*-a na mobilni uređaj prije same ekstrakcije podataka. U slučajevima kada pregled ili prikupljanje podataka nije moguće obaviti bez promjene konfiguracije uređaja, postupak i promjene moraju se ispitati, potvrditi i dokumentirati. Slijeđenje odgovarajuće metodologije i smjernica ključno je u ispitivanju mobilnih uređaja jer se tako u većini slučajeva dolazi do najveće količine podataka. Kao i kod svakog prikupljanja i analiziranja dokaza, nepoštivanje odgovarajućeg postupka tijekom ispitivanja može rezultirati gubitkom ili oštećenjem dokaza, a može ga učiniti nedopuštenim i neprihvatljivim na sudu, [10].

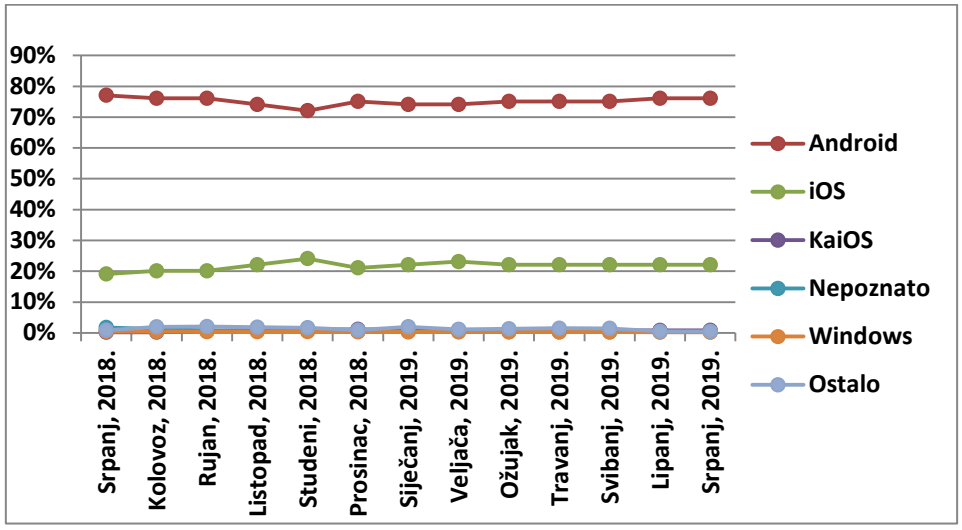
2.2.1. Funkcionalnosti mobilnih terminalnih uređaja

Mobilni uređaji dinamični su sustavi koji forenzičkom istražitelju pružaju mnoge izazove u izdvajanju i analizi digitalnih dokaza, koji će biti detaljno objašnjeni u nastavku. Važno je naglasiti da se pod pojmom mobilnih uređaja ne smatraju samo mobilni telefoni već svi uređaji koji imaju vlastitu memoriju i mogućnost komuniciranja. To uključuje PDA (eng. *Personal Digital Assistant*) uređaje, GPS (engl. Global Positioning System) uređaje, tablete, novije igraće konzole, i sl., [12]. Brzo povećanje broja različitih vrsta i proizvođača mobilnih uređaja otežava razvoj jednog procesa ili alata za ispitivanje i analiziranje svih vrsta uređaja. Mobilni uređaji neprestano se razvijaju kako napreduju postojeće tehnologije te kako se razvijaju i uvode nove tehnologije. Svaki mobilni uređaj dizajniran je s različitim ugrađenim operativnim sustavima stoga forenzički stručnjaci moraju posjedovati posebna znanja i vještine kako bi mogli provesti prikupljanje i analizu podataka za različite uređaje, [10].

Postoji nekoliko različitih tehnologija mobilnih uređaja koje se koriste, uključujući GSM (engl. *Global System for Mobile Communications*), CDMA (engl. *Code Division Multiple Access*), TDMA (engl. *Time Division Multiple Access*) te iDEN (engl. *Integrated Digital Enhanced Network*). Najčešći od njih je GSM koji se koristi u velikom broju mobilnih uređaja, a CDMA ima veliku prisutnost u SAD-u. Ostale tehnologije se koriste, no nisu toliko zastupljene kao dvije navedene. Postoji mnogo varijabli u GSM i CDMA tehnologijama kao

što su veličina i frekvencija ćelija. Jedna razlika je u tome što susjedne ćelije u CDMA mreži mogu koristiti istu frekvenciju pa je omogućena meka primopredaja signala između ćelija jer poziv može imati više veza. Kada se poziv prenosi između ćelija, prvo uspostavlja se jača veza, a zatim slabija. Nasuprot tome GSM se oslanja na tvrdu primopredaju što znači da se za poziv koristi samo jedan kanal. GSM uređaji koriste modul pretplatničkog identiteta, poznatog kao SIM kartica (engl *Subscriber Identity Module*). SIM kartica povezuje uređaj s mrežom i može se mijenjati između uređaja. SIM kartica može biti zanimljiva forenzičkim istražiteljima jer često sadrži značajne informacije kao što su adresar i konfiguracijski podaci. Također, ne manje važni su podaci o identitetu pretplatnika, a to su IMEI (engl. *International Mobile Equipment Identity*) i ESN (engl. *Electronic Serial Number*). Ovi brojevi ili kodovi često su prikazani na naljepnici na uređaju, a mogu biti važni za utvrđivanje identiteta korisnika tijekom forenzičkih istraga, [3].

Za forenzičke istrage vrlo je važno odrediti na kojem operativnom sustavu uređaj radi. U današnje vrijeme postoje mnogobrojni proizvođači te mnogobrojni različiti operativni sustavi. Najčešće korišteni su Android i iOS, a forenzički istražitelji morali bi poznavati i ostale operativne sustave kako ne bi došlo do problema prilikom forenzičkih istraga. Forenzički istražitelji moraju gotovo svu pažnju posvetiti softverskom dijelu uređaja obzirom da su noviji uređaji po hardverskim specifikacijama vrlo slični. U nastavku je prikazana statistika korištenja pojedinih operativnih sustava diljem svijeta, [6].



Grafikon 1: Statistika o korištenju uređaja prema operativnim sustavima
Izvor: [13]

Grafikon 1 prikazuje statistiku korištenja mobilnih uređaja prema njihovim operativnim sustavima. Vidljivo je da su mobilni uređaji temeljeni na Android operativnim sustavima najkorišteniji uređaji, a njihov udio u svim mobilnim uređajima diljem svijeta je 76,03 %. Drugi najkorišteniji operativni sustav je iOS, a njegov udio u svim mobilnim uređajima diljem svijeta je 22,04%. U Republici Hrvatskoj situacija je veoma slična, a postotak uređaja koji je temeljen na Android operativnim sustavima je 83,5% dok uređaji temeljeni na iOS-u čine 15,45% svih mobilnih uređaja. Udio ostalih operativnih sustava je izrazito nizak što je vidljivo na prethodnoj slici.

2.2.2. Potreba za mobilnom forenzikom

Forenzika pametnih mobilnih uređaja relativno je novo i brzo rastuće područje digitalne forenzike te dobiva primjenu u brojnim kriminalističkim istragama kao i unutar policije. Današnji mobilni uređaji postaju pametniji, jeftiniji i lako dostupni običnom čovjeku za svakodnevnu upotrebu, [5].

Brzo razvijajuća industrija mobilnih uređaja dosegla je nezamisliv vrhunac. Budući da mnogi mobilni uređaji postaju snažni i funkcionalni kao osobna računala, za očekivati je da će ih isti zamijeniti u skorijoj budućnosti. Na dnevnoj osnovi svaki pametni mobilni uređaj prikuplja veliki broj osjetljivih podataka koji se odnose na njegovog vlasnika, a što može predstavljati spremište podataka koji mogu biti značajni u rješavanju mnogobrojnih pitanja. Danas se pametni mobilni uređaji koriste za obavljanje gotovo svih zadataka koji su se u prošlosti obavljali na tradicionalne načine. To se odnosi na tradicionalne zadatke koji uključuju slanje i primanje poziva, kratke tekstualne poruke i e-mailove pa sve do složenijih zadataka, npr. geolokacija, provjera stanja računa, provođenje bankarskih transakcija, zadataka upravljanja, i sl. S obzirom na tempo kojim razvoj uređaja i tehnologija napreduje, potreba za razvojem i napretkom forenzike je neizbježna. Podaci pohranjeni u mobilnim uređajima neprestano postaju bogatiji i relevantniji što je djelomično posljedica eksplodirajućeg rasta i korištenja mobilnih aplikacija kao i društvenih mreža. Povrh toga, svi mobilni uređaji mogu pohranjivati sve vrste osobnih podataka, a to se u većini slučajeva događa nenamjerno, [14]. Broj mobilnih uređaja diljem svijeta je 4,68 milijardi, a svaki od tih uređaja može potencijalno predstavljati prijetnju te je iz tog razloga mobilna forenzika izrazito važna i njena potreba je neupitna, [15].

Mobilna forenzika važna je iz jednostavnog razloga, a to je da kupnja pametnog mobilnog uređaja znači stjecanje podataka o svakodnevnom životu vlasnika odnosno korisnika mobilnog uređaja. Neki proaktivni pristupi stjecanju odnosno prikupljanju podataka dobivaju mjesto u kriminalnom kontekstu ne samo nakon zločina, nego i kada ljudi krše propise i zakone kao što je sprječavanje terorističkih pokušaja, zločina protiv države i pedofilije. U današnje vrijeme važnost mobilne forenzike uspostavljena je i ne može se više zanemariti jer je svaki pojedinačni bajt važan i može puno značiti u forenzičkim istragama, [14].

2.2.3. Izazovi mobilne forenzike

Ne postoji veći izazov za digitalnog forenzičkog istražitelja od mobilne forenzike. Mobilni uređaji imaju mnogo jednakih mogućnosti kao potpuno funkcionalni računalni sustav (primjerice igre, fotografije, razmjene poruka i mogućnost slanja multimedije), [16]. Za razliku od tradicionalne računalne forenzičke istrage, mobilne forenzičke vještine postaju vrlo tražene u današnjim istraživanjima zbog brojnih činjenica koje čine prikupljanje digitalnih dokaza iz mobilnih uređaja vrlo složenim zadatkom. To može biti posljedica svakodnevnih

ažuriranja koji se pojavljuju u mobilnim operativnim sustavima, raznolikosti standarda, tehnologiji pohrane podataka i postupcima zaštite podataka. Za razliku od računalnog istraživanja, mobilna istraga se teško može standardizirati. Za svaki pojedini model uređaja, a prema uslugama koje se stavljaju na raspolaganje korisniku u mobilnoj forenzici razlikuje se vrlo velik raspon kategorija dokaza, [14].

Forenzički ispitivači suočavaju se s raznim izazovima, a mobilni uređaj koristi se kao izvor dokaza. Na mjestu zločina, ako je mobilni uređaj pronađen isključen, ispitivač bi ga trebao staviti u Faraday vrećicu/torbu kako bi spriječio moguće promjene ako se uređaj sam uključi. Ako je uređaj pronađen uključen isključivanje bi moglo nanijeti određene posljedice, stoga je taj korak nužno izbjeći. Ako je uređaj zaključan PIN-om ili lozinkom ili je šifriran, ispitivač će morati zaobići zaključavanje ili odrediti PIN za pristup uređaju koristeći brojne alate i tehnike. Mobilni uređaji su mrežni uređaji i mogu slati i primati podatke putem različitih izvora kao što su telekomunikacijski sustavi, Wi-Fi pristupne točke i *Bluetooth*. Ako je moguće potrebno je izvršiti odspajanje mobilnog uređaja od mreže prije stavljanja u Faraday torbu u svrhu zaštite dokaza. To će također sačuvati bateriju uređaja koji se nalazi u Faraday torbi jer se uređaj neće truditi povezati na bilo koju mrežu. Jedan od najvećih forenzičkih izazova kada je u pitanju mobilna platforma je činjenica da se podacima može pristupiti te da se oni mogu pohraniti i sinkronizirati na više uređaja. Budući da su podaci nestabilni i mogu se brzo preoblikovati ili brisati na daljinu, potrebno je više napora za očuvanje tih podataka.

Forenzičari često imaju poteškoće u prikupljanju digitalnih dokaza s mobilnih uređaja, a slijede neki od razloga:

- **Hardverske razlike –** U današnje vrijeme tržište mobilnih uređaja preplavljeno je brojnim različitim modelima i proizvođačima. Forenzički ispitivači mogu se prilikom provođenja forenzičke analize susresti s različitim vrstama mobilnih uređaja koji se razlikuju po veličini, hardveru, značajkama i operativnom sustavu, [10]. Po definiciji pametni mobilni uređaj je prijenosni uređaj i namijenjen je širokom skupu funkcionalnosti. Hardverska arhitektura pametnih telefona značajno se razlikuje od računala i također varira od proizvođača mobilnih uređaja do korisnika. Pametni mobilni uređaji obično se sastoje od mikroprocesora, matične ploče, ROM i RAM memorije, zaslona osjetljivog na dodir , radijskog modula i / ili antene, mikrofona i zvučnika, digitalne kamere i GPS uređaja. Isti proizvođač obično proizvodi visoko prilagođene operativne sustave kako bi odgovarao specifikacijama hardvera. Zbog velikog broja raznolikosti u hardveru forenzički ispitivači moraju koristiti velik broj dodatnih adaptera i kablova, [14].
- **Mobilni operativni sustavi** - Mobilni uređaji koriste više vrsta operativnih sustava kao što su Apple's iOS, Google's Android, RIM's, BlackBerry OS, Microsoft's Windows Mobile, HP's webOS, Nokia's Symbian OS i mnogi drugi, [10]. Ažuriranja operativnog sustava su vrlo česta među dobavljačima, a velika ažuriranja obično se objavljuju u svakom tromjesečju. Iz tog razloga potrebno je pratiti promjene na tržištu, a ovaj problem naglašen je činjenicom da glavni razvojni inženjeri i razvojni forenzički alati razmatraju svoju poslovnu tajnu razvoja i ne objavljuju informacije o

niskim razinama njihovih kodova. Osim toga, ispitivanje "manje uobičajenih" operativnih sustava, kao što je Windows Phone, zahtijeva puno forenzičkog iskustva, [14].

- **Sigurnosne značajke mobilne platforme -** Moderne mobilne platforme sadrže ugrađene sigurnosne značajke za zaštitu korisničkih podataka i privatnosti. Ove značajke djeluju kao prepreka tijekom fizičke ekstrakcije podataka. Na primjer, moderni mobilni uređaji dolaze sa zadanim mehanizmima enkripcije od hardverskog sloja do softverskog sloja. Ispitivač bi možda trebao proći kroz ove mehanizme šifriranja kako bi ekstrahirao podatke s uređaja. Te sigurnosne značajke mogu varirati od jednostavnih četveroznamenkastih PIN-ova do složenijih i dugačkih lozinki, a mogu se sastojati i od zaključavanja uzorkom. Novi modeli mobilnih uređaja mogu imati zaključavanje pomoću otiska prsta ili biometrije za identifikaciju korisnika, [10].
- **Razlike u datotečnim sustavima** – Različiti operativni sustavi i hardveri mobilnih uređaja podrazumijevaju različite načine pohranjivanja podataka i pokretanja različitih datotečnih sustava. Primjerice, ista aplikacija koja radi na Android-u, razlikuje se od slične aplikacije koja se izvodi na iOS-u. Ta činjenica znatno komplicira dekodiranje, parsiranje i rezbarenje informacija (engl. *Carving*). Razlike u datotečnim sustavima znače da forenzički alati neće moći obraditi neke datoteke i da se moraju vrlo često ažurirati, [14].
- **Nedostatak resursa -** S rastućim brojem mobilnih uređaja alati koje zahtijevaju forenzički ispitivači također bi se povećali. Forenzički pribor kao što su USB kabeli, baterije i punjači za različite mobilne uređaje moraju se održavati kako bi uspješno istraživali uređaje. Forenzički ispitivači moraju neprestano pratiti trendove razvoja novih forenzičkih alata te se opskrbljivati njima.
- **Generičko stanje uređaja -** Čak i ako se čini da je uređaj izvan stanja rada, pozadinski procesi mogu i dalje raditi. Na primjer, u većini mobilnih uređaja budilica i dalje radi čak i kad je uređaj isključen. Nagli prijelaz iz jedne države u drugu može rezultirati gubitkom ili promjenom podataka. Ovo je vrlo bitno za forenzičke istražitelje jer u mnogim slučajevima mobilni uređaj zapisuje podatke o korisniku bez njegova znanja.
- **Nestabilnost podataka** - Puno važnih dokaznih podataka nalazi se u pametnom mobilnom uređaju na nestabilan način, što rezultira provođenjem rasprava prilikom forenzičke analize mobilnog uređaja. Pametni mobilni uređaji dodaju ovo ograničenje forenzičarima; zaplijenjeni uređaji moraju biti uključeni i izolirani kako bi se spriječio gubitak podataka ili prepisivanje postojećih podataka, [14].
- **Komunikacijska zaštita -** Mobilni uređaji komuniciraju putem mobilnih mreža, Wi-Fi mreža, Bluetooth i infracrvene mreže. Kako komunikacija uređaja može promijeniti podatke na uređaju potrebno je ukloniti mogućnost daljnje komunikacije. Najčešći primjer komunikacijske zaštite je Faraday torba.
- **Nedostatak dostupnosti alata -** Postoji širok raspon mobilnih uređaja. Jedan alat možda ne podržava sve uređaje ili obavlja sve potrebne funkcije pa treba koristiti kombinaciju alata. Odabir odgovarajućeg alata za određeni mobilni uređaj može

predstavljati dugotrajni proces jer je potrebno ispitati koji alat ima mogućnost ekstrakcije najveće količine podataka s promatranog uređaja.

- **Zlonamjerni programi -** Uređaj može sadržavati zlonamjerni softver poput virusa ili trojanskog konja. Takvi zlonamjerni programi mogu se pokušati proširiti na druge uređaje preko žičnog sučelja ili bežičnog uređaja.
- **Pravna pitanja -** Mobilni uređaji mogu biti uključeni u zločine koji mogu prelaziti zemljopisne granice. Kako bi se riješila ova pitanja pravde, forenzički ispitivač treba biti svjestan prirode zločina i regionalnih zakona, [10].

Forenzički istražitelji susreću se i s problemom oblaka. Radi memorije, uštede prostora za pohranu, ili zbog sigurnosnih kopija, današnji uređaji pohranjuju mnogo važnih podataka na oblaku. Većina dobavljača nudi memorijski prostor besplatno, a podaci se u većini slučajeva automatski sinkroniziraju s nekim računom u oblaku. Android podaci šalju se Googleu, podaci za iPhone šalju se u iCloud, a podaci sustava Windows Phone sinkroniziraju se s uslugom OneDrive. Osim toga, neke usluge trećih strana također nude određeni memorijski prostor besplatno, kao što je Dropbox. U nekim slučajevima prikupljanje dokaza nije nužno tehnički zadatak, nego prije svega pravni zadatak jer zahtjevi se moraju rješavati uslugama pohrane u oblaku kako bi se mogli primiti željeni podaci, [17].

2.2.4. Mobilni terminalni uređaji kao izvor podataka

Mobilni terminalni uređaji postali su sastavni dio svakodnevnog života ljudi te su kao takvi skloni olakšavanju kriminalnih aktivnosti ili mogu biti na neke druge načine uključeni u zločine. Ni jedan drugi uređaj nije toliko „osoban“ kao što je mobilni uređaj, a razlog tomu je što se stalno nalazi blizu vlasnika te u velikoj većini slučajeva pripada pojedincu, [3]. Informacije pohranjene na mobilnim uređajima te one koje su povezane s mobilnim uređajima mogu pomoći u rješavanju ključnih pitanja u istrazi, otkrivajući s kim je pojedinac bio u kontaktu, o čemu su komunicirali i gdje su bili, [17].

Proizvođači mobilnih uređaja obično nude slične značajke i mogućnosti upravljanja informacijama, uključujući aplikacije za upravljanje osobnim informacijama (engl. *Personal Information Management*, PIM), poruke, e-poštu, pregledavanje web-a, i sl. Značajke i mogućnosti razlikuju se ovisno o razdoblju u kojem je uređaj izrađen, izmjenama koje su napravljene te aplikacijama koje je instalirao korisnik [18]. U nastavku su navedeni izvori podataka koje je moguće ekstrahirati iz mobilnih uređaja:

- **SIM kartica** – SIM (engl. *Subscriber Identity Module*) kartica neophodni je dio svakog mobilnog uređaja, a upotrebljava se s GSM i iDEN mrežama. Omogućuje korisnicima manipulaciju podataka imenika i poruka te korisničke autentifikacije među mobilnim uređajima. Ekstrakcija SIM kartice može dobaviti vrlo bitne podatke za istragu, kao što su: telefonski brojevi upućenih/primljenih poziva, kontakti, pojedinosti o SMS-u (vrijeme, datum, primatelj, itd.) te sami tekst poruke, [9].

- **Lokacije** – Sposobnost određivanja lokacije mobilnih uređaja postala je snažna istraživačka sposobnost. Postoje dvije kategorije informacija koje mobilni uređaj s GPS sposobnosti može pružiti forenzičkim ispitivačima. Prva kategorija su informacije o razini sustava, a druga su podaci stvoreni od strane korisnika. Informacije o razini sustava odnose se na zapise koje mobilni uređaj sam bilježi, neovisno o korisniku. Podaci stvoreni od strane korisnika podrazumijevaju korisničku interakciju, a odnose se na upisane rute, lokacije i putne točke. Ekstrakcija lokacija iz mobilnih uređaja može dati korisne informacije za istragu, a neke od njih su: zapisnici tragova, putne točke, rute, pohranjene lokacije, sigurnosne lokacije, nedavne adrese, i sl., [19].
- **E-pošta** – Elektronička pošta koristi se kao dokazni materijal u većini forenzičkih istraga. Ona se sastoji od tri glavna dijela, a to su: izvorišna adresa, odredišna adresa te sami tekst poruke, odnosno datoteke koje se prenose. Potencijalni izvori informacija koji se mogu pronaći ekstrakcijom e-pošte su: privitci s ekstenzijama kao što su .doc, .xls, ili slike, ljudi odnosno adrese koje su navedene u CC-u (engl. *Carbon Copy*), ljudi odnosno adrese kojima je poruka proslijeđena te originalne poruke, [9].
- **Digitalna kamera** – Digitalna kamera može biti od velikog značaja za forenzičke istrage jer može sadržavati fotografije ili videozapise koji mogu riješiti određeni slučaj. Forenzička analiza digitalne kamere, odnosno fotografija ili videozapisa koji su njome nastali dijeli se u dvije grane, a to su prepoznavanje i identifikacija izvora slike. Postupak forenzičke analize nad digitalnom kamerom može pribaviti mnoge značajne podatke, kao što su: lokacija snimljene fotografije ili videozapisa, datum i vrijeme snimljene fotografije ili videozapisa te veličinu i ekstenziju fotografije ili videozapisa, [20].
- **Internetski preglednici** – Pretraživanje digitalnih dokaza koji su ostavljeni aktivnošću pregledavanja Interneta također može biti ključna komponenta digitalnih forenzičkih istraga. Svaki pokret ili aktivnost korisnika ostaje zapisana na mobilnom uređaju, stoga forenzički istražitelji trebaju posvetiti veliku pažnju ovom izvoru potencijalnih dokaza. Forenzička analiza internetskih preglednika uključuje sve podatke koji se mogu otkriti o korisničkoj aktivnosti na Internetu, a tu se mogu pronaći poruke e-pošte, preuzete datoteke, popis posjećenih stranica, lozinke, i sl. Forenzičkom analizom internetskih preglednika mogu se prikupiti korisne informacije za istragu, kao što su: povijest posjećenih stranica, kolačići, ključne riječi, preuzete ili pokrenute datoteke, lozinke, itd, [21].
- **SMS** – SMS (engl. *Short Message Service***)** je usluga koju mobilni uređaji koriste za slanje kratkih poruka između uređaja. U današnje vrijeme sve se manje koristi, no ne treba ju izuzeti iz forenzičkih istraga jer može sadržavati komunikaciju osumnjičenih osoba. Većina današnjih forenzičkih alata usmjerenih mobilnim uređajima ekstrahiraju SMS poruke, a one uključuju sami tekst poruke, pošiljatelja i primatelja te datum i vrijeme slanja, [22].
- **Zapisnici poziva** – Zapisnici poziva dolaze iz dva različita izvora. Jedan izvor odnosi se na pozive u osumnjičenikovom uređaju, a drugi se odnose na pozive

zapisane u dnevniku koji se vode kod telekom operatora ili pružatelja mobilne mreže. Puno pouzdaniji izvor zapisnika poziva su pozivi zapisani kod telekom operatora jer pozivi koji se nalaze na osumnjičenikovom uređaju vrlo lako mogu biti manipulirani. Zapisnici poziva predstavljaju privatne evidencije o aktivnostima korisnika, a telekom operatori služe za čuvanje povjerljivosti tih evidencija s izuzetkom objavljivanja ako zakon to nalaže. Zapisi poziva mogu razriješiti razne slučajeve u forenzičkim istragama. Pritom se analiziraju sljedeći podaci: datum i vrijeme poziva, trajanje poziva, učestalost uspostave poziva, broj pozivatelja, favorite, preslušavanje obavljenog razgovora, itd, [23].

- **Društvene mreže** – U današnje vrijeme gotovo svaki korisnik mobilnih uređaja koristi minimalno jedan oblik društvenih mreža. To korištenje također predstavlja potencijalno veliku količinu digitalnih dokaza koji mogu biti korisni za razne forenzičke istrage. Forenzička istraživanja društvenih mreža znaju biti jako kompleksna, no podaci koji se mogu ekstrahirati mogu biti izrazito osjetljivi. Forenzička analiza društvenih mreža može ekstrahirati podatke kao što su: osobni podaci, komunikacija između korisnika, zadnje aktivno vrijeme, objave koje se sviđaju korisniku, prijatelji, i sl., [24] .
- **Memorijske kartice** - Memorijske kartice služe za proširenje memorijskog prostora na mobilnom uređaju. Kao i memorija unutar uređaja, ova vrsta memorije može sadržavati značajan set podataka ključnih za istragu. Provođenje forenzičke analize nad memorijskim karticama zahtijeva njihovo uklanjanje te posebnu obradu, [25].

2.3. Antiforenzika

Digitalna antiforenzika je pojam novijeg datuma i produkt je digitalne forenzike kao znanstvene, pravne i tehničke kategorije. Poznato je da je digitalna forenzika skup metoda, tehnika i pravila koja imaju za cilj provođenje istrage nad digitalnim medijima, a u svrhu tumačenja elektroničkih podataka. Kao što samo ime kaže, antiforenzika predstavlja suprotnost forenzici, a ona predstavlja skup tehnika, postupaka i pravila koja imaju za cilj negativno utjecati na postojanje, količinu i/ili kvalitetu digitalnih dokaza te pokušati ili onemogućiti pregled i analizu dokaza, [26]. Garfinkel (2007.) je istaknuo da je antiforenzika skup alata i tehnika kojima se ometaju forenzički alati, istrage i forenzički istražitelji. Peron i Legary (2005.) definiraju antiforenziku kao pokušaj ograničavanja identifikacije, prikupljanja, uspoređivanja i validacije elektroničkih podataka, [3].

Postoje mnogi ciljevi antiforenzike, ovisno o određenom slučaju ili osobi, a primarni ciljevi prema [27] su:

- Izbjegavanje detekcije određenih događaja
- Povećanje vremena provedbe forenzičke analize i istrage
- Ometanje prikupljanja informacija
- Osporavanje forenzičkog izvještaja ili svjedočenja na sudu

- Otkrivanje prisutnosti forenzičkih alata
- Iskorištavanje nedostataka forenzičkih alata za napad na sustav

2.3.1. Antiforenzičke metode

Antiforenzičke metode mogu se klasificirati u više skupina, ovisno o primjeni ili načinu korištenja, o načinu rada tih metoda i ovisno o tome na koji način utječu na postojeće forenzičke metode, alate i tragove. Svrha i cilj antiforenzičkih metoda nije uvijek zlonamjerna, poput skrivanja tragova napada, skrivanja zapisa koji mogu dovesti forenzičkog istražitelja do napadača ili brisanja podataka, nego se antiforenzikom može ukazati na greške u radu forenzičkih istražitelja, na slabosti određenih forenzičkih alata te se njome može potaknuti razvoj i poboljšanje postojećih alata. Isto tako, može služiti kao metoda obrane od krađe podataka, jer na jednak način kako se forenzički alati mogu koristiti u dobre svrhe, isto tako se mogu koristiti i u zlonamjerne svrhe, [28].

Najprihvaćenija i najčešća podjela antiforenzičkih metoda je sljedeća, a detaljnije je opisana u nastavku odjeljka:

- Skrivanje podataka
- Brisanje podataka
- Skrivanje tragova
- Napadi na forenzičke alate

Skrivanje podataka je proces kojim se osjetljivi podaci za forenzičku istragu skrivaju kako bi se proces otkrivanja tih podataka otežao, ali i da ti podaci mogu biti dostupni i prikazani osobi koja im je pokušala zametnuti trag. Jednostavan primjer ovog postupka je smještanje dokumenata koji se žele sakriti u neku regularnu datoteku koja ima naziv koji će odvući forenzičkog istražitelja, na primjer osjetljive slike se premještaju u datoteku pod nazivom „Materijali za fakultet“, [26]. Ova tehnika ne pokušava uništiti niti manipulirati dokazima, već je to pokušaj da podaci odnosno dokazi budu manje vidljivi tijekom procesa forenzičke istrage. Datoteke bi se mogle skrivati u običnom obliku kako bi se iskorištavale slijepe točke istražitelja ili unutar drugih datoteka kako bi se iskoristila naslijeđena ograničenja forenzičkog softvera, [3].

Jedan od načina skrivanja podataka je steganografija. Osnovni princip steganografije je prikrivanje samog postojanja informacije koja se prenosi unutar nekog naizgled bezazlenog medija ili skupa podataka. Moderna steganografija koristi prednosti digitalne tehnologije, a najčešće podrazumijeva skrivanje tajne poruke unutar neke multimedijske datoteke, kao što su slike, audio ili video datoteke. Razlog tomu je što multimedijske datoteke sadrže neupotrebljene podatkovne prostore koje steganografske metode i tehnike koriste tako da ih popune tajnim informacijama, [29]. Drugi, i možda najpoznatiji način skrivanja podataka je kriptografija. Osnovni cilj kriptografije je omogućiti sigurnu komunikaciju putem nesigurnog medija, odnosno komunikacijskog kanala, tako da treća osoba ne može razumjeti

komunikaciju, [30]. Dobar način skrivanja podataka je i čista eliminacija izvora podataka. Moguće je upotrijebiti različite programe koji pakiraju skriveni i zlonamjerni kod u sebi, dođu do mete napada te otpakiraju taj zlonamjerni kod, [28].

Brisanje podataka jedna je od najčešćih antiforenzičkih metoda. U ovu metodu također spada i fizičko uništavanje ili demagnetiziranje diskova kako bi se obrisali svi tragovi ikakvog postojanja podataka. Postoje različiti načini sigurnog brisanja podataka, od jednostavnog prepisivanja novih podataka preko postojećih, do višestrukog pisanja točno određenih vrijednosti na sektore diska a u cilju onemogućavanja povratka na početne podatke u kojima se mogu nalaziti potencijalni tragovi određenog napada, [28].

Kao što je navedeno, jedan od načina sigurnog brisanja podataka je demagnetiziranje diskova. Kod demagnetiziranja koristi se uređaj koji se zove demagnetizator. On prilikom procesa demagnetiziranja briše i postavke formatiranja niske razine koje su postavljene u proizvodnji diska, [28]. Međutim, potencijalni problem kod demagnetizacije diskova može predstavljati cijena demagnetizatora, no ako je ulog vrijedan potrošenog novca, osoba koja bi željela uništiti podatke koji bi mogli dovesti do velike kazne naći će novac za demagnetizator, [26]. Također, jedan od načina je fizičko uništavanje diska, uređaja ili medija. Fizičko uništavanje može se provesti na razne načine, a neki od njih su paljenje diska, usitnjavanje, razbijanje, otapanje u kiselinama, i sl., [28].

Skrivanje tragova metoda je čija je svrha zavarati, dezorijentirati i preusmjeriti proces forenzičke istrage. Cilj je sakriti tragove identiteta napadača te tragove aktivnosti koje je ostavio u sustavu. Obuhvaća razne tehnike i alate koji uključuju čišćenje log-ova, *spoofing* (metoda za zamjenu IP adresa), trojanske konje, i sl. Jedan od najpoznatijih alata je *Timestomp* (dio *Metasploit Framework*-a) koji omogućuje korisniku da mijenja datoteke s metapodacima koji se odnose na pristup, kreiranje i modifikaciju datuma/vremena. Korištenjem ovog alata korisnik može renderirati (postupak stvaranja slika) bilo koji broj datoteka, čineći ih beskorisnima u pravnom smislu, jer se dovodi u pitanje njihov kredibilitet, [31].

Način prikrivanja tragova i skrivanja pravih podataka napada moguće je ostvariti lažiranjem podataka. Napadač može lažirati podatke o napadu, postaviti lažne podatke napada, napraviti dodatne datoteke koje nemaju posebnu funkciju, te na taj način pokušati maknuti sumnju sa sebe te odvesti forenzičkog istražitelja u krivom smjeru. Ova metoda je vrlo efikasna osobito ako je pred zakonom potrebno dokazati da je napadač izmijenio vremena pristupa datotekama, [28].

Napadi na forenzičke alate podrazumijevaju napade i iskorištavanje forenzičkih alata koje koriste forenzički istražitelji u digitalnim istragama, na način da se sakriju aktivnosti, promijene neke sistemske vrijednosti, i sl. Jedan od načina je korištenje alata koji brišu sve tragove aktivnosti korisnika kako na samom uređaju tako i na Internetu, [32].

Djelovanje protiv digitalnih forenzičkih alata predstavlja direktne napade na proces digitalne forenzike. Napadi na forenzičke alate imaju potencijal uzrokovati izrazito negativne učinke na forenzičku istragu. Napadi se izvode zato što se forenzički alati ne razvijaju za rad u

nesigurnom okruženju i isključuju pretpostavku da će se na njih izvršiti napad. Također, forenzički alati nisu zaštićeni od prijetnji, a korisnici forenzičkih alata, odnosno forenzički istražitelji ne provode testiranja robusnosti, pouzdanosti i funkcionalnosti alata prije kupnje, ali upravo na sve te navedene razloge je potrebno obratiti veliku pažnju jer napadi mogu uzrokovati ogromne posljedice, [27].

2.3.2. Mobilna antiforenzika

Današnji mobilni uređaji mogu se poistovjetiti s računalima jer imaju gotovo sve njihove karakteristike. Mobilni uređaji opremljeni su grafičkim sučeljem, računalnim resursima, mogućnošću povezivanja te pohranom velike količine podataka. Na mobilnim uređajima pohranjuje se velika količina osobnih podataka što ih čini savršenim ciljem za forenzičke istrage. Neke od tradicionalnih antiforenzičkih tehnika nisu uvijek primjenjive na mobilni svijet.

Postoje različite antiforenzičke tehnike usmjerene mobilnim platformama, a to su, [3]:

- **Mobilni unutarnji akvizicijski alat (MIAT, engl. *Mobile internal acquisition tool*)**– Pomoću MIAT-a istražitelji bi lakše mogli formulirati bolji antiforenzički plan. Može se koristiti kao proaktivna mjera pronalaženja dokaza/podataka koji su ostavljeni na mobilnom uređaju.
- **Iskorištavanje Android značajki** – Android povezuje bilo koju pokrenutu aplikaciju sa sigurnim Sandboxom[1] koji ne može ometati druge aplikacije bez izričitog dopuštenja. Dozvole se definiraju jednom statički tijekom instalacije aplikacije i ne mijenjaju se tijekom rada aplikacije. Zaštita je osigurana na razini operativnog sustava, dakle, služi kao antiforenzička tehnika.
- **Privatne mape** – Može se stvoriti sigurna privatna mapa u koju se mogu pohranjivati tekstualne datoteke i multimedijski sadržaji. Stvorena mapa bi mogla biti skrivena od drugih aplikacija koji osiguravaju određenu razinu steganografije.
- **Antiforenzička aplikacija** – AFDroid je aplikacija koja stvara privatnu mapu, ali također omogućuje izvršavanje dva procesa. Prvi od njih je EEP (engl. *Evidence Export Process)* odnosno izvozni proces dokaza koji omogućuje izvoz informacija pohranjenih na mobilnom uređaju na privatnu lokaciju. Drugi proces je EIP (engl. *Evidence Import Process*) odnosno uvozni postupak dokaza koji vrši obrnutu radnju od EEP-a.
- **Uništavanje dokaza** – Ako je potrebno uništiti privatnu mapu, potrebno je deinstalirati aplikaciju AFDroid. Korištenje značajki tvorničkog vraćanja podataka briše neke podatke, ali opet neki podaci mogu i ostati na uređaju.

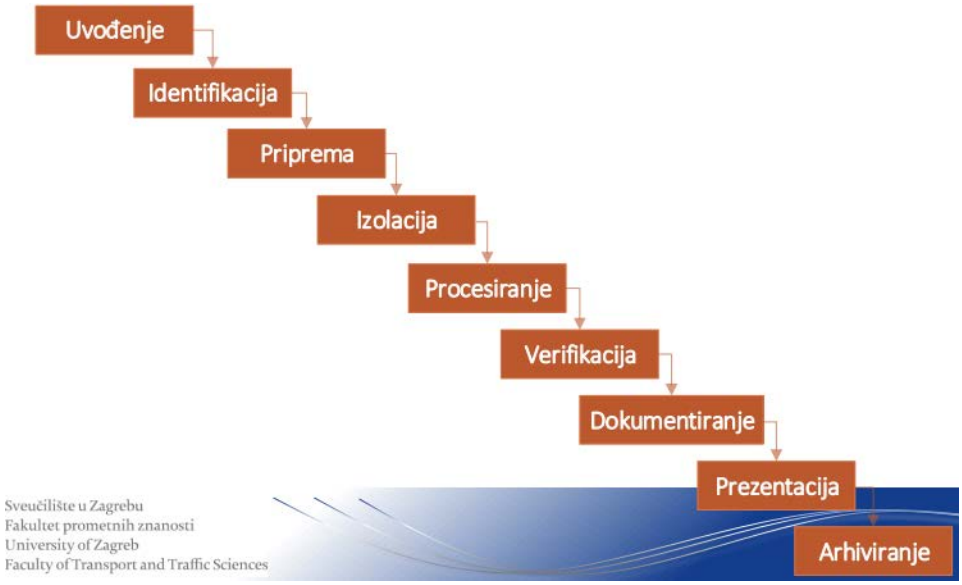
[1] Sandbox – sigurnosni mehanizam za odvajanje pokrenutih programa, obično u pokušaju ublažavanja kvarova sustava ili širenja softverskih ranjivosti

3. Sistematizacija metoda i postupaka ekstrakcije podataka

Ekstrakcija podataka predstavlja radnju ili postupak dohvaćanja podataka iz različitih izvora ili medija (koji su uglavnom loše strukturirani), a u cilju daljnje obrade i pohrane. Cilj ekstrakcije podataka je doći do podataka do kojih se ne može doći klasičnim pregledavanjem uređaja, a koji mogu biti korisni u rješavanju određenih kriminalističkih slučajeva, [14]. Ona ovisi o količini i vrsti podataka koji se žele ekstrahirati, a provodi se različitim metodama, alatima te postupcima uz slijeđenje referentnih faza ekstrakcije podataka, što je detaljno objašnjeno u nastavku poglavlja, [33].

3.1. Faze ekstrakcije podataka

Svako ekstrahiranje digitalnih dokaza i forenzičko ispitivanje mobilnog terminalnog uređaja može se razlikovati. Naime, ako se slijede pravilni postupci i koristi pravilan pristup za ekstrakciju podataka mobilnih uređaja, do potrebnih podataka dolazi se puno jednostavnije. Međutim, iako se trebaju slijediti određeni postupci i faze, ne postoji uspostavljen standardni postupak za mobilnu forenziku. Sve metode koje se koriste prilikom ekstrakcije podataka mobilnih uređaja moraju biti testirane, validirane i dobro dokumentirane. Sljedeća slika daje pregled faza ekstrakcije podataka koji će se naknadno opisati.



Slika 1: Faze ekstrakcije podataka, [1]

Faza uvođenja dokaza početna je faza procesa ekstrakcije podataka i ona uključuje postupke kojima se rješavaju zahtjevi za ispitivanje. Ova faza u pravilu uključuje obrasce zahtjeva, papirologiju te potrebnu dokumentaciju lanca čuvanja dokaza (engl. *Chain of Custody*), informacije o vlasništvu i vrstu incidenta u koju je mobilni uređaj bio uključen, a navode se i opće informacije o vrsti podataka koje podnositelj zahtjeva želi ekstrahirati ili

dokumentirati iz mobilnog terminalnog uređaja. Kritični aspekt u ovoj fazi ispitivanja je razvoj specifičnih zahtjeva za svako ispitivanje, [34].

Faza identifikacije druga je faza ekstrakcije podataka, a u njoj forenzički istražitelji moraju identificirati brojne pojedinosti za svaki pregled mobilnog uređaja, a to su:

- **Pravno ovlaštenje za pregled mobilnog uređaja** – Od izrazite je važnosti jer forenzički istražitelj mora utvrditi i dokumentirati zakonska ovlaštenja koja se odnose na pristup i pregledavanje mobilnog uređaja, kao i na sva druga ograničenja koja se postavljaju na uređaj prije pregleda, [10]
- **Ciljevi ispitivanja** - Odnose se na istražiteljevo utvrđivanje koliko detaljno se forenzičko ispitivanje mora provesti, odnosno na kojim podacima se treba temeljiti. Ciljevi ispitivanja mogu imati značajnu ulogu u odabiru alata i tehnika u forenzici mobilnih uređaja. Opći proces koji se koristi za ispitivanje bilo kojeg mobilnog uređaja trebao bi biti prikupljanje što više informacija, a cilj ispitivanja za svaki mobilni uređaj može biti drugačiji. Cilj ispitivanja može alternativno uključiti pokušaj obnavljanja izbrisanih podataka iz memorije mobilnog uređaja. Također, ciljevi mogu napraviti značajnu razliku u korištenju alata i tehnika za ispitivanje mobilnog uređaja, [34].
- **Izraditi, identificirati i modelirati podatke za uređaj** – Pomaže pri određivanju alata koji će raditi s uređajem, [10]. To omogućuje ispitivaču ne samo da kasnije identificira određeni mobilni uređaj, nego pomaže i u određivanju o tome koji alati mogu raditi s mobilnim uređajem, a koji ne, jer većina forenzičkih alata mobilnih uređaja nudi popise podržanih uređaja na temelju proizvođača i modela uređaja. Za sve uređaje potrebno je identificirati i dokumentirati proizvođača, broj modela, serijski broj te trenutni telefonski broj, [34].
- **Promjenjiva i dodatna pohrana podataka** – Mobilni uređaji omogućuju proširenje memorije s izmjenjivim, odnosno prijenosnim uređajima za pohranu kao što je „Micro SD kartica“. Ako se tijekom forenzičkog ispitivanja takva kartica pronađe u uređaju, nju je potrebno ukloniti i obraditi pomoću tradicionalnih forenzičkih tehnika, [10]. Osim toga, mobilni uređaji mogu omogućiti vanjsko pohranjivanje podataka unutar područja za pohranu temeljenih na mreži, a primjer toga je *Cloud* pohrana, [34].
- **Ostali izvori potencijalnih dokaza** - Osim navedenih pojedinosti, važno je uzeti u obzir i ostale izvore potencijalnih dokaza. Mobilni uređaji mogu biti dobri izvori otiska prsta i drugih bioloških dokaza. Izvori otiska mogu se pronaći na zaslonu mobilnog uređaja jer oni često služe kao način otključavanja mobilnog uređaja. Takvi dokazi trebali bi biti prikupljeni prije ispitivanja mobilnog uređaja kako bi se izbjegla kontaminacija, odnosno, da ispitivač ostavi svoje tragove na zaslonu, [10].

Faza pripreme je faza gdje se uključuju istraživanja vezana za određeni mobilni uređaj koji se ispituje te se uključuju razni alati koji će se koristiti za pregled tog uređaja. Određuju se mogućnosti i metode ekstrakcije podataka koje bi se trebale primjenjivati u daljnjim koracima ekstrakcije. Faza pripreme uključuje specifična istraživanja o određenim mobilnim uređajima koji će se ispitivati. Nakon što je identifikacija modela uspješno provedena, forenzički ispitivač može dalje istraživati određeni mobilni uređaj kako bi utvrdio

koji su alati dostupni za ekstrakciju podataka. Forenzički alati koji su prikladni za ispitivanje mobilnog uređaja bit će određeni čimbenicima kao što su cilj ispitivanja, vrsta mobilnog uređaja te prisutnost bilo kakvih vanjskih mogućnosti pohrane, [34].

Faza izolacije usmjerena je zaštiti mobilnih uređaja od komunikacije i pristupa raznim mrežama. Mobilni uređaji dizajnirani su za različite načine komuniciranja, kao što su mobilne mreže, Bluetooth, infracrvene tehnologije, NFC, itd. Kada je mobilni uređaj povezan na neku mrežu, odnosno komunicira putem navedenih tehnologija, postoji mogućnost da će doći novi podaci koji mogu promijeniti dokaze u uređaju. Uređaji se izoliraju kako bi se onemogućilo mijenjanje podataka u slučaju komunikacije te uništenje podataka daljinskim pristupom.

Izolacija uređaja može se ostvariti uporabom Faraday vrećice koja blokira radio signale prema uređajima. Također, jedan od načina je postavljanje antene za zaštitu frekvencija ili postavljanje uređaja u zrakoplovni način rada, [10]. Metode kao što su smještanje uređaja u Faraday vrećicu ili postavljanje uređaja u zrakoplovni način rada mogu imati i potencijalne probleme. Naime, kada se uređaji izoliraju, teško je, ili nemoguće raditi s mobilnim uređajem jer se oni ne mogu vidjeti ili se ne može pristupiti tipkovnici. Nažalost, nemaju svi mobilni uređaji zrakoplovni način rada, a uz to, ponekad i najizglednije metode izolacije mogu propasti. Čak i ako je mobilni uređaj uspješno izoliran od svih mreža postoji mogućnost utjecaja na korisničke podatke, kao što su alarmi ili podsjetnici za sastanke. Ako dođe do takvih situacija, forenzički ispitivač treba dokumentirati svoje pokušaje izolacije mobilnog uređaja kao i pojavu dolaznih poziva, tekstualnih poruka ili drugih prijenosnih podataka, [34].

Slika 2: Izolacija mobilnog uređaja korištenjem Faraday vrećice, [35]

Faza procesiranja ili obrade mobilnog uređaja trebala bi se odvijati korištenjem potvrđenih i testiranih metoda koje su ponovljive. Uz korištenje adekvatnih metoda, potrebno je koristiti učinkovite i testirane alate za ekstrakciju podataka kako bi se postigli definirani ciljevi istrage. Postoje brojne metode za ekstrakciju podataka koje će biti objašnjene u nastavku. Jedna od metoda koja je poželjna je fizička ekstrakcija jer ima najveću moć u ekstrakciji podataka te ekstrahira podatke iz sirove memorije. Ako fizička ekstrakcija bude neuspješna, potrebno je primijeniti ostale metode kako bi se došlo do željenih podataka, [10].

Unutar faze procesiranja pristupa se podacima pohranjenim na memorijskim karticama. Pristup podacima na memorijskim karticama može promijeniti podatke stoga bi se ona trebala ukloniti iz mobilnog uređaja te bi trebala biti odvojeno obrađena pomoću tradicionalnih metoda digitalne forenzike. Povrh toga, SIM kartice bi trebale biti odvojene od mobilnog uređaja i njih bi se trebalo posebno obrađivati, [34].

Faza verifikacije odnosi se na potvrdu točnosti ekstrahiranih podataka u svrhu njihovog osiguravanja, odnosno kako bi se onemogućila njihova potencijalna izmjena. Provjera ekstrahiranih podataka može se izvršiti na nekoliko načina, a to su:

- **Usporedbom ekstrahiranih podataka i podataka na uređaju** – Vrlo je važno provjeriti jesu li ekstrahirani podaci iz mobilnog uređaja jednaki onima u uređaju. Ekstrahirani podaci se mogu uspoređivati sa samim uređajem ili logičkim izvješćem, ovisno što se traži i što je poželjno. Preporučuje se izbjegavanje rukovanja mobilnim uređajem jer to može uzrokovati promjenu digitalnih dokaza, [10].
- **Upotreba više alata i uspoređivanje dobivenih rezultata** – Drugi način da se osigura točnost ekstrahiranih podataka je korištenje više od jednog alata za ekstrakciju podataka iz mobilnih uređaja i provjera rezultata analizom ekstrakcije različitih alata. Ako postoje nedosljednosti, forenzički ispitivač treba koristiti druga sredstava kako bi se provjerila točnost podataka, [34].
- **Upotreba hash vrijednosti** – Sve datoteke trebaju biti zaštićene, odnosno kriptirane nakon ekstrakcije kako bi podaci ostali nepromijenjeni. Ako je moguće provesti ekstrakciju datotečnog sustava, ispitivač ekstrahira datotečni sustav te izračunava zaštite za ekstrahirane datoteke. Kasnije se svaka pojedinačno ekstrahirana zaštićena datoteka izračunava i provjerava prema izvornoj vrijednosti u svrhu provjere njene cjelovitosti. Svako odstupanje hash vrijednosti mora biti zabilježeno i detaljno objašnjeno, [10].

Faza dokumentiranja je faza kod koje je forenzički ispitivač dužan dokumentirati postupak ekstrakcije u obliku bilješki koje se odnose na cjelokupni rad koji je proveden nad određenim mobilnim uređajem. Nakon što istraga završi, rezultati moraju proći kroz određene recenzije kako bi se provjerilo jesu li zadovoljavajući, odnosno je li istraga u konačnici dovršena. Dokumentacija o pregledavanju uređaja trebala bi se odvijati tijekom cijelog postupka istraživanja, [34].

Bilješke i dokumentacija ispitivača treba sadržavati informacije kao što su:

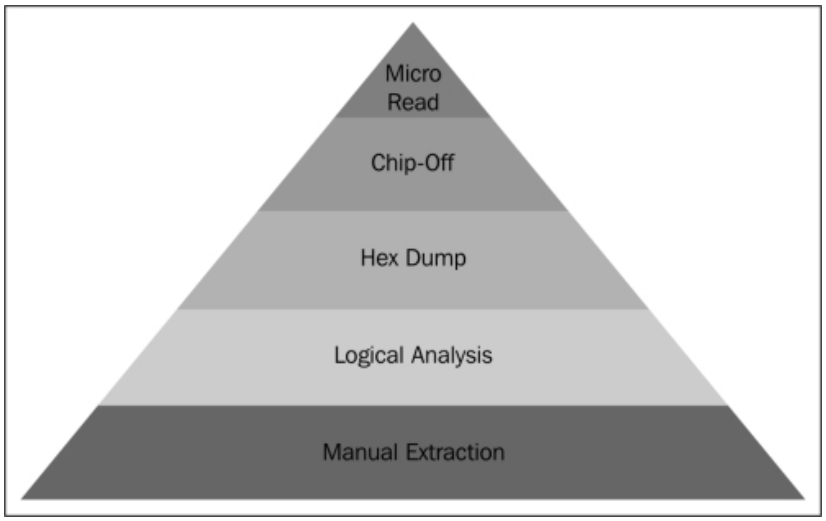
- Datum i vrijeme početka ispitivanja
- Fizičko stanje mobilnog uređaja
- Fotografije mobilnog uređaja i pojedinih komponenti (npr. SIM kartica i memorijska kartica)
- Status mobilnog uređaja kada je zaprimljen (uključen ili isključen)
- Model uređaja
- Alati koji se koriste za ekstrakciju
- Pronađeni podaci tijekom ispitivanja, [10]

Faza prezentacije slijedi nakon faze dokumentacije, a u ovoj fazi je naglasak upravo na prezentaciji tih dokumentiranih podataka. Ona osigurava jasan prikaz rezultata dobivenih istragom drugom istražitelju, tužitelju, sudu ili odgovornoj osobi. Vrlo je važno izraditi forenzičko izvješće o ekstrahiranim podacima iz mobilnog uređaja tijekom ekstrakcije ili analize. To može uključivati podatke u papirnatom ili digitalnom obliku. Rezultati provedene istrage moraju biti jasni, sažeti, koncizni i ponovljivi. Analiza vremenske linije koja prikazuje vremenski slijed događanja te značajki koje nude komercijalni alati za forenzičku analizu mogu pomoći u izvještavanju i objašnjavanju nalaza za više mobilnih uređaja. Ekstrahirane tekstualne poruke mogu također biti dokaz u sudskim postupcima, ali fotografije iste tekstualne poruke mogu biti vizualno uvjerljivije, [10]. Često je vrlo korisno prikazati niz slika tekstualnih poruka i zapisnika povijesti poziva u kronološkom redoslijedu putem jednostavnih prezentacija tako da se ekstrahirani podaci jasno prikažu publici, bez obzira je li publika istražitelj, tužitelj ili neka treća strana. To je posebno učinkovito ako postoji određeni broj mobilnih uređaja koji su uključeni u slučaj, [36].

Faza arhiviranja, odnosno faza pohrane zadnja je faza u ekstrakciji podataka mobilnih uređaja koja nije manje važna od ostalih faza. Važan dio cjelokupnog procesa ekstrakcije podataka je očuvanje ekstrahiranih i dokumentiranih podataka. Također, vrlo je važno da se podaci čuvaju u upotrebljivom obliku za sudski proces koji je u tijeku ili za neke buduće sudske postupke, [10]. Neki sudski postupci mogu potrajati i nekoliko godina prije konačnog rješenja, a većina jurisdikcija zahtijeva da se podaci čuvaju u različitim vremenskim razmacima za potrebe žalbe. Poradi vlasničke prirode različitih alata na tržištu za izdvajanje i dokumentiranje podataka o mobilnom uređaju, potrebno je razmotriti mogućnost kasnijeg pristupanja spremljenim podacima. Ako je moguće, podaci bi se trebali pohraniti na standardne medije u standardnim formatima kako bi se kasnije moglo pristupiti podacima čak i ako izvorni forenzički alat više nije dostupan. Također dobra praksa može biti zadržavanje kopije samog alata kako bi se olakšalo pregledavanje podataka kasnije, [34].

3.2. Metode ekstrakcije podataka

Ekstrakcija podataka u prvom redu ovisi o veličini i količini podataka koju forenzički istražitelj mora ekstrahirati. Prilikom ekstrakcije podataka potrebno je odabrati odgovarajuću metodu, no u velikom broju slučajeva potrebno je koristiti kombinaciju različitih metoda ekstrakcija. Najjednostavnijim i najlakše izvedivim metodama ekstrakcije dolazi se do najmanje količine podataka i tu se ostvaruje najmanja efikasnost. Naravno, u usporedbi s jednostavnim metodama kompleksnije i zahtjevnije metode daju najveću efikasnost, odnosno njima se dolazi do najveće količine podataka te skrivenih ili izbrisanih podataka. Kod kompleksnih metoda ekstrakcije sam postupak je vrlo kompliciran i dugotrajan te zahtijeva velike financijske izdatke. Sljedeća slika prikazuje piramidu ekstrakcije podataka, [37].



Slika 3: Metode ekstrakcije podataka, [10]

Slika 3 prikazuje piramidu metoda ekstrakcije podataka, gdje donji dio piramide čine metode koje nisu tehnički zahtjevne i ne zahtijevaju složene forenzičke alate i postupke. Gornji dio piramide čine metode koje su izrazito zahtjevne i zahtijevaju velike financijske izdatke kao i obučenost forenzičkih istražitelja u područjima hardvera mobilnih uređaja te poznavanja načina na koji mobilni uređaji rade, a te metode spadaju u fizčke ekstrakcije. Dobar forenzički istražitelj mora moći odrediti koji alat će koristiti za koju metodu ekstrakcije podataka jer nisu svi alati podržani za sve načine ekstrakcije. Također, što je metoda viša na piramidi ona postaje teža za opravdati odnosno objasniti te njen postupak traje puno duže negoli metode koje se nalaze na dnu piramide, [10].

3.2.1. Osnovne metode ekstrakcije podataka

3.2.1.1. Ručna ekstrakcija

Ručna ekstrakcija podataka (engl. *Manual Extraction*) najjednostavniji je način prikupljanja odnosno ekstrakcije podataka s mobilnih uređaja. Ona predstavlja izravnu interakciju forenzičkog istražitelja s mobilnim uređajem te njegovu manipulaciju samim uređajem, kao što je to korištenje mobilnih uređaja od strane običnih korisnika, [12]. Manipulacija uređaja odnosi se na pregledavanje pohranjenog sadržaja na uređaju manipulacijom fizičkih komponenti kao što su tipkovnica ili zaslon osjetljiv na dodir. Ručna ekstrakcija može se provoditi samo ako je mobilni uređaj otključan te ne zahtijeva dodatna stručna znanja forenzičkog istražitelja za upravljanje procesom ekstrakcije, [33]. Sva interakcija s mobilnim uređajem mora biti zabilježena, a često se koriste digitalne kamere. Tijekom ručne ekstrakcije mijenja se stanje uređaja jer svaki korak forenzičkog istražitelja ostaje zapisan u memoriji uređaja, a iz tog razloga potrebno je minimizirati korake prilikom manipulacije uređajem, [12]. Forenzički istražitelj pregledava mobilni uređaj, njegove

postavke te sav sadržaj koji je dostupan i običnom korisniku, koristeći navigaciju kroz datotečni sustav koji mobilni uređaj pruža svojim grafičkim sučeljem, [10].

Ručna ekstrakcija ima jednu veliku prednost, a to je mogućnost uporabe na gotovo svim mobilnim uređajima, neovisno o njegovom proizvođaču. Prednost ručne ekstrakcije je i jednostavnost uporabe, odnosno rukovanja jer ne zahtijeva dodatna osposobljavanja i posebna znanja forenzičkih istražitelja što omogućuje jednostavnost uporabe i mogućnost brze ekstrakcije podataka. Uzevši u obzir sve činjenice, ručna ekstrakcija ipak nije efikasna metoda ekstrakcije podataka jer ne može pristupiti svim podacima na mobilnom uređaju, što je apsolutno neprihvatljivo za bitnije forenzičke istrage. Jedan od problema može biti i jezik na kojem uređaj radi jer ga forenzički istražitelj možda neće poznavati, a razlog tomu je što ručna ekstrakcija ne pruža platformu na svim jezicima. Nedostatak ručne ekstrakcije može biti i neispravan ili oštećen mobilni uređaj, odnosno njegov zaslon osjetljiv na dodir, jer postoji mogućnost da određene funkcije neće raditi i provedba forenzičkog ispitivanja neće biti moguća. Problem ručne ekstrakcije je i što ne može očuvati integritet uređaja te ne može pristupiti skrivenim i obrisanim podacima, [37].

3.2.1.2. Logička ekstrakcija

Logička ekstrakcija podataka predstavlja proces povezivanja mobilnog uređaja s forenzičkom radnom stanicom putem bežične ili žičane veze. Forenzička postaja, odnosno radna stanica je sklopovlje, posebni uređaj ili stolno računalo koje je pripremljeno za provođenje forenzičke analize nad mobilnim uređajima, [12]. U svrhu povezivanja mobilnog uređaja i forenzičke radne stanice mogu se koristiti povezivanja putem USB (engl. *Universal Serial Bus*) kabela, RJ-45 (engl. *Registered Jack 45*) kabela, infracrvene te *Bluetooth* tehnologije. Ova vrsta ekstrakcije podataka se uglavnom odvija korištenjem tvorničkog sučelja mobilnog uređaja, a služi za sinkroniziranje podataka s osobnim računalom. Postupak logičke ekstrakcije zasniva se na slanju naredbe od strane računala prema mobilnom uređaju te interpretiranju te naredbe od strane mobilnog uređaja. Nakon toga, traženi podaci primaju se iz memorije uređaja i šalju prema forenzičkoj radnoj stanici, a forenzički ispitivač kasnije može pregledati podatke. Trenutno većina dostupnih forenzičkih alata podržava izvođenje logičke ekstrakcije, [10].

Dvije su osnovne vrste logičke ekstrakcije podataka, a to su:

- **Agentski temeljena ekstrakcija** (engl. *Agent based*) – Zasniva se na instalaciji „agenta“ na uređaj koji je predmet istrage odnosno s kojeg se žele ekstrahirati podaci, a agent predstavlja određeni softver ili aplikaciju. Nakon što je agent instaliran na uređaju, podaci se ekstrahiraju, a nakon uspješne ekstrakcije agent se briše odnosno deinstalira.
- **Ekstrakcija korištenjem ADB naredbi** (engl. *Android Debug Bridge*) – Zasniva se na komunikaciji s uređajem za preuzimanje odnosno ekstrakciju podataka s uređaja. Prilikom ovakve vrste ekstrakcije potrebno je da mobilni uređaj ima uključeno USB

ispravljanje pogrešaka. Ukoliko je uređaj zaključan i USB ispravljanje pogrešaka nije omogućeno, ADB naredbe neće moći dohvatiti rezultate, [33].

Logička ekstrakcija se na većini forenzičkih alata izvodi tako da se prvo stvori sigurnosna kopija mobilnog uređaja, a onda se na toj kopiji provodi logička ekstrakcija. U većini slučajeva, forenzički alati koji provode logičku ekstrakciju, ekstrahiraju puno veću količinu podataka ako je na mobilnom uređaju omogućen *root* pristup. U sljedećim poglavljima bit će prikazana usporedba ekstrakcije podataka s uređaja na kojemu je ostvaren *root* pristup te uređaja na kojemu nema *root* pristupa, [12].

Najveće prednosti logičke ekstrakcije su brzina izvođenja te jednostavnost uporabe. Ona nije kompliciranа za korištenje te ima mogućnost ekstrakcije različitih informacija, a količina tih informacija puno je veća nego li je to u ručnoj ekstrakciji. Podržava velik broj stranih jezika što predstavlja olakšanje i jednostavnost forenzičkom istražitelju. Kod logičke ekstrakcije izrazito je važna ponovljivost, odnosno mogućnost izvođenja neograničen broj puta. Jedan od problema logičke ekstrakcije je mogućnost izmjene ili zanemarivanja određenih podataka, kao što je to nepročitani SMS. Nedostatak je i potreba za velikim brojem kablova koji se koriste za povezivanje s uređajem. U većini slučajeva logička ekstrakcija ne prikuplja izbrisane podatke, no to ovisi o uređaju i ostvarenom pristupu na njemu. Problem predstavlja zaštićeni i zaključani uređaj, jer sama logička ekstrakcija nema mogućnost probijanja takvog uređaja i morale bi se koristiti različite metode kako bi se uređaj otključao te omogućio za izvođenje logičke ekstrakcije podataka, [37].

3.2.1.3. Datotečna ekstrakcija

Između logičke i fizičke metode, nalazi se datotečna ekstrakcija podataka. Razlog zašto se datotečna ekstrakcija smješta između ove dvije je količina prikupljenih podataka koja je manja nego li je to u fizičkoj ekstrakciji, a veća nego li je to u logičkoj ekstrakciji podataka. Može se reći da je datotečna ekstrakcija dio ili podskup logičke ekstrakcije, a ona koristi metode s drugačijim skupom protokola, u ovisnosti o operativnom sustavu. Obuhvaća sve datoteke koje su pohranjene na dijelu memorije koji se smatraju zauzetima, odnosno popunjenima. Glavna namjena datotečne ekstrakcije je prikaz rasporeda sustava, odnosno datoteka koje se nalaze na mobilnom uređaju. Datotečna ekstrakcija može se provoditi putem SQL naredbi stoga forenzički istražitelj mora biti educiran i u tom području. Pri zapisivanju podataka na memoriju samog uređaja, adresa memorije smatra se zauzetom sve dok korisnik mobilnog uređaja ne obriše podatke. Iako se u tom slučaju smatra da se podaci brišu, zapravo se briše samo adresa podataka. Datotečna ekstrakcija može unutar datoteka pronaći i nevidljive informacije kao što su obrisani sadržaji, privremeni sadržaji te ostaci prijašnjih datoteka. Podaci koji se dobivaju datotečnom ekstrakcijom su uglavnom baze podataka aplikacija, sistemski podaci, log zapisi, povijesti pretraživanja, itd, [33] .

Najčešće metode koje se koriste u datotečnoj ekstrakciji su:

- ADB (engl. *Android Debug Bridge*)
- Android Backup
- Android Backup APK downgrade

Prednost datotečne ekstrakcije je što prikazuje detaljnu strukturu mobilnog uređaja te datoteka koje su pohranjene na njemu. Također, može ekstrahirati vrlo korisne informacije kao što su povijesti pretraživanja te promjene unutar sustava mobilnog uređaja. Problem može predstavljati SQL jezik, ako forenzički istražitelj nije dovoljno educiran u tom području. Najveći nedostatak datotečne ekstrakcije je nemogućnost pristupa podacima nakon formatiranja memorije uređaja. Također, ako su podaci pohranjeni na nedodijeljenom odnosno nealociranom dijelu memorije, datotečna ekstrakcija ih neće moći pronaći, [38].

3.2.1.4. Fizička ekstrakcija

Fizička ekstrakcija najzahtjevnija je i najteže izvediva metoda ekstrakcije podataka. Izvršava se povezivanjem mobilnog uređaja s forenzičkom radnom stanicom, a ta forenzička radna stanica je u velikoj većini slučajeva osobno računalo. Nakon povezivanja mobilnog uređaja s forenzičkom radnom stanica upisuje se kod ili se pokreće sustav mobilnog uređaja te ga se upućuje da isporuči memoriju s mobilnog uređaja na forenzičku radnu stanicu. Fizička ekstrakcija je najopsežnija, ali najmanje podržana metoda ekstrakcije podataka. Najmanje je podržana jer zahtijeva potpuni pristup unutarnjoj memoriji mobilnog uređaja, a taj pristup ovisi o operativnom sustavu i sigurnosnim mjerama koje određuju proizvođači mobilnih uređaja, [39]. Podaci koji se dobivaju fizičkom ekstrakcijom uglavnom su u obliku slike koja je u binarnom formatu stoga je potrebna tehnička stručnost za analizu. Fizička ekstrakcija podrazumijeva kopiranje svakog bita (*bit-by-bit*) koji se nalazi na cijelom fizičkom mediju na kojem se vrši analiza. Fizička ekstrakcija upotrebljava se kada je potrebna kompletna forenzička analiza mobilnog uređaja. Koristi napredne metode ekstrakcije fizičke *bit-by-bit* slike *flash* memorije mobilnog uređaja. Fizička ekstrakcija jedna je od najzahtjevnijih jer je potrebno zaobići sigurnosne mehanizme koji omogućuju pristup samom uređaju na kojem je medij pohranjen te manipulaciju podataka, a iz tog razloga je rijetko dostupna u besplatnim forenzičkim alatima.

Fizička ekstrakcija se može podijeliti u dvije glavne kategorije, a to su invazivna i neinvazivna fizička ekstrakcija. Invazivna fizička ekstrakcija podrazumijeva fizičko rastavljanje, odnosno otvaranje uređaja, s pristupom SoC-u, matičnoj ploči ili memorijskim modulima, a u tu svrhu se najčešće koriste JTAG, Chip Off te Micro Read koje će biti detaljnije objašnjene u nastavku. Drugu kategoriju čine neinvazivne metode fizičke ekstrakcije koje ne zahtijevaju fizičko rastavljanje, odnosno otvaranje uređaja. U tu svrhu primjenjuju se metode kao što su *Client*, ADB, *Bootloader*, *Forensic Recovery Partition*. U većini slučajeva poseže se za invazivnim metodama jer se njima može pronaći veća količina podataka, [33].

Najvažnija prednost fizičke ekstrakcije je ekstrahiranje izbrisanih podataka. Također, ekstrahira podatke koji su skriveni iz izbornika datotečnih sustava što može predstavljati koristan trag jer se iz skrivenih podataka vrlo često mogu razotkriti zlonamjerne radnje. Fizičku ekstrakciju od ostalih metoda ekstrakcije razlikuje mogućnost zaobilaska ili probijanja zaporki čime se može zaključiti da je fizička ekstrakcija najučinkovitija metoda ekstrakcije podataka. Kao i sve ostale metode ekstrakcije i fizička ekstrakcija ima nedostatke. Nedostatak predstavljaju teška ekstrakcija podataka i dugo vrijeme trajanja ekstrakcije. Također, puno je veća količina podataka za dekodiranje i interpretaciju i zahtijeva velika znanja forenzičkih istražitelja. Fizičku ekstrakciju nije moguće provesti na svim uređajima pa je potrebno koristiti ostale metode ekstrakcije podataka prije fizičke ekstrakcije, ukoliko je to moguće, [37].

3.2.1.4.1. Hex Dump

Hex Dump jedna je od metoda fizičke ekstrakcije sirovih podataka pohranjenih u *flash* memoriji uređaja. Postiže se povezivanjem uređaja s forenzičkom radnom stanicom i upisivanjem nepotpisanog koda za isporuku podataka s mobilnog uređaja na forenzičku radnu stanicu ili računalo. Svaki od tih kodova nosi instrukcije za preuzimanje memorije s mobilnog uređaja na forenzičku radnu stanicu, kako je prethodno i navedeno. Rezultirajuća sirova slika je u binarnom formatu stoga je potrebna tehnička stručnost za njenu analizu, [10]. U većini slučajeva potrebno je da su mobilni uređaji *flasher*, odnosno da omogućavaju manipuliranje *flash* memorije na uređaju. To predstavlja prednost forenzičkom ispitivaču jer takvi uređaji omogućuju odlaganje memorije uređaja. Za ovu metodu ekstrakcije podataka razvijeni su brojni specijalizirani forenzički alati iako se ova metoda ne upotrebljava u velikom broju slučajeva. Uređaji na kojima je moguće provesti *Hex Dump* metodu omogućuju snimanje memorije mobilnog uređaja kao slike. Ta se slika tada može pregledati na isti način kao i svaka druga slika na računalu. Proces provođenja ove metode ekstrakcije nije skup, daje veliku količinu podataka forenzičkom istražitelju te dopušta oporavak izbrisanih podataka s uređaja koji su pohranjeni na nedodijeljenim dijelovima memorije, [40].

3.2.1.4.2. JTAG

JTAG (engl. *Joint Test Action Group*) je udruga elektroničkih industrija koja je osnovana 1985. godine u svrhu razvijanja metoda provjera dizajna i ispitivanja tiskanih pločica nakon izrade. On može biti zanimljiv forenzičkim istražiteljima i analitičarima jer može pružiti izravan pristup memoriji mobilnog uređaja, bez ikakve šanse da ga on promijeni, [17].

Provođenje forenzičke analize JTAG metodom spada u fizičke invazivne metode jer je potrebno otvaranje mobilnog uređaja. JTAG je napredna metoda sakupljanja podataka koja uključuje povezivanje s pristupnim točkama (TAP, engl. *Test Access Ports*) na uređaju te

upućivanje procesora da prenese neobrađene podatke na povezanim memorijskim čipovima. Ako je podržan, JTAG je izuzetno učinkovita metoda koju binarna inteligencija koristi za ekstrahiranje cjelovite fizičke slike s uređaja, a što nije moguće dobiti uobičajenim forenzičkim alatima. Koristi se i kada je utor za prijenos podataka nedostupan. Većina slučajeva gdje se JTAG primjenjuje uključuje mobilne uređaje koje rade na Android operativnim sustavima te uređaje koji su zaključani uzorkom i ne mogu se zaobići, [41]. U većini slučajeva za uspješnu ekstrakciju podataka potrebno je ukloniti bateriju mobilnog uređaja kako bi se moglo pristupiti procesoru, a za tu radnju se koristi vanjsko napajanje, [42].

JTAG metoda ekstrakcije podataka u velikoj većini slučajeva je učinkovita, odnosno ekstrahira veliku količinu podataka. Važno je naglasiti da je ključna prednost JTAG metode mogućnost ekstrakcije podataka koji su izbrisani ili prikriveni. Njome se zaobilaze lozinke, uzorci i svi sustavi zaštite na razini grafičkog sučelja mobilnog uređaja. Osim navedenih prednosti, JTAG posjeduje i velike nedostatke. Veliki problem je što JTAG zahtijeva pretvorbu podataka, a što jako odužuje proces ekstrakcije podataka. Metoda je ograničena na određeni broj uređaja, a provedba ekstrakcije može biti različita za pojedine uređaje. Također, metoda je zahtjevna i spora jer je potrebna dodatna oprema i veliki broj kablova, a forenzički istražitelji moraju pažljivo rukovati procesorom i pinovima kako se oni ne bi oštetili, [37].

3.2.1.4.3. Chip-Off

Chip-Off fizička je metoda ekstrakcije podataka mobilnih uređaja kod koje se ekstrakcija podataka vrši direktno s memorijskog čipa uređaja. Uključuje fizičko uklanjanje memorijskih čipova iz uređaja, a ekstrakcija i pregled podataka pohranjenih na njima vrši se s različitim čitačima čipova ili drugim uređajima koji se koriste za ekstrahiranje podataka. Ova metoda je tehnički najzahtjevnija metoda, a njena provedba može potrajati jako dugo i može zahtijevati velike financijske izdatke jer mobilni uređaji sadrže veliki broj čipova. Ona se koristi kada su sve ostale metode isprobane, a učinka nije bilo, [41]. Vrlo je važno da su forenzički istražitelji koji provode ekstrakciju podataka ovom metodom dobro obučeni, jer nepravilni postupci mogu oštetiti memorijski čip i tako učiniti podatke nečitljivima i neupotrebljivima. Spada u učinkovite, ali izrazito destruktivne metode ekstrakcije podataka pa je forenzički istražitelji ne primjenjuju ako na to nisu primorani, [43]. Informacije koje se ekstrahiraju u osnovnom su formatu i potrebno ih je analizirati, dekodirati i tumačiti. Može se koristiti kada je uređaj oštećen, a memorijski čip netaknut, [41].

Ova metoda ekstrakcije podataka izrazito je učinkovita i njena velika prednost je što može ekstrahirati sve vrste podataka iz mobilnih uređaja. Pruža dobar prikaz događanja u uređaju koji može biti vrlo koristan za forenzičke istrage. Također, zaobilazi sve sigurnosne mehanizme osim enkripcije podataka, no i taj problem se može riješiti tako da se direktno iz memorije sazna enkripcijski ključ. Velika prednost je što zadržava integritet podataka i pruža mogućnost ekstrakcije podataka iz oštećenog uređaja te radi sa svim vrstama memorije. Problem može predstavljati mjesto gdje se podaci nalaze, odnosno podaci ne moraju biti blizu jedni drugih što može usporiti proces ekstrakcije podataka. Također, ekstrahirani podaci nisu

u standardnim formatima pa je potrebna njihova pretvorba kako bi se mogli razumjeti i analizirati. Tijekom procesa ekstrakcije moguće je oštećenje čipova, a to može rezultirati gubitkom podataka. Zahtijeva velika ulaganja u opremu te korištenje velikog broja kablova, [37].

Slika 4: Prikaz odvajanja čipa s matične ploče mobilnog uređaja, [44]

3.2.1.4.4. Micro Read

Micro Read je metoda koja uključuje ručno pregledavanje i tumačenje podataka vidljivih na memorijskim čipovima. U tu svrhu forenzički ispitivači koriste elektronski mikroskop s kojime analiziraju fizičke ulaze na čip, a zatim prevodi status vrata na 0 i 1 kako bi se odredili odgovarajući ASCII znakovi. Cijeli proces je dugotrajan i skup te zahtijeva posebna znanja i obuku na *flash* memoriji i datotečnom sustavu. Uz to, metoda je jako spora i zahtijeva skupu i složenu tehničku opremu, a to je elektronski mikroskop. Također, potreban je niz stručnjaka koji moraju biti obučeni za rad na takvoj opremi. Zbog izrazito velike složenosti cijelog procesa, *Micro Read* se ne koristi za klasične forenzičke slučajeve, već se eventualno može koristiti za slučajeve koji ugrožavaju nacionalnu sigurnost ili neke druge slučajeve takve važnosti. Forenzički istražitelji koji provode ovu vrstu ekstrakcije podataka (uz poznavanje rada na elektronskom mikroskopu) moraju vrlo dobro poznavati građu uređaja. Trenutno ne postoje komercijalni alati za izvođenje ove vrste ekstrakcije podataka. Ova metoda se smatra zastarjelom i napuštenom jer su tijekom vremena metode nižih razina uznapredovale i u većini slučajeva su dovoljne za ekstrakciju željenih podataka s uređaja. Prednost ove metode ekstrakcije je mogućnost izdvajanja svih podataka iz memorije uređaja, kao i dobra slika o onome što se događa unutar mobilnog uređaja, [10]. Kao što je navedeno, ova metoda ekstrakcije nije poželjna, a neki od njenih nedostataka su velika cijena, izrazito zahtijevan proces ekstrakcije, dugotrajna ekstrakcija te nepostojeći formati izvješća, [37].

3.2.1.4.5. ISP eMMC

ISP (engl. *In-System Programming*) metoda je usmjerena uređajima koji sadrže eMMC (engl. *Embedded MultiMedia Controller*) *flash* čipove odnosno module. To su *flash* čipovi koji integriraju *flash* memoriju i kontroler u jedan modul. U modernim mobilnim uređajima uobičajeno su u 2 – 128 GB. Ova metoda vrlo je slična JTAG metodi samo su vodiči povezani na specifične točke vezane uz memorijski modul. ISP eMMC je metoda koja je manje invazivna u odnosu na *Chip-Off* metodu no invazivnija od JTAG metode, [45]. Koristi se radi preuzimanja kompletnog memorijskog sadržaja uređaja. ISP omogućuje forenzičkom ispitivaču isplativija forenzička ispitivanja stoga se ova metoda ne smije zanemariti, [46]. Ova tehnika je korisna iz nekoliko razloga, a jedan je da neki mobilni uređaji nemaju pristupne TAP-ove ili je proizvođač onemogućio pristup podacima putem TAP-a. Da bi se ovaj problem zaobišao, potrebno je lemiti žice na otpornike i kondenzatore koje omogućuju pristup. To znači da se ovim postupkom zaobilazi procesor uređaja dok izravno čita komponentu. Ova tehnika može biti izuzetno učinkovita te omogućiti ekstrakciju cjelovite fizičke slike uređaja, a da se ne mora pribjegavati destruktivnom postupku čipiranja. Nakon dovršetka forenzičke analize, mobilni uređaj se može ponovno sastaviti i normalno funkcionirati, [47].

3.2.2. Ostale metode ekstrakcije podataka

3.2.2.1. Flasher Box

Flasher Box jedna je od metoda ekstrakcija podataka koja se koristi ako prethodno navedene metode nisu dostupne, odnosno ako se traži jeftinije rješenje. To su mali uređaji koji su izvorno dizajnirani s namjerom servisiranja ili nadogradnje mobilnih uređaja. Pomažu forenzičkim istražiteljima osiguravati komunikaciju s mobilnim uređajem koristeći dijagnostičke protokole za komunikaciju s memorijskim čipom, [18]. Te kutije predstavljaju alternativno rješenje u forenzičkoj analizi, a mogu pomoći u prevladavanju ograničenja komercijalnih alata po pitanju troškova. Nisu *forensically sound* te predstavljaju opasnost za integritet podataka zato što nisu zamišljene kao sredstvo za forenzičku analizu. Kutije se povezuju s računalom preko USB-a i mobilnog uređaja koji se analiziraju putem posebnih kabela koji na kutiji obično implementiraju standardni RJ-45 utor. Kao i kod ostalih komercijalnih alata, ova metoda uključuje niz posebnih kabela, ali za razliku od njih, ovi kablovi se mogu kupiti s različitih internetskih trgovina. Još jedan razlog zašto ova metoda nije *forensically sound* je što neke od sposobnosti *Flasher Box*-ova nisu sasvim legalne, [48].

Flasher Box potpuno dohvaća izbrisane i prikrivene sadržaje i to mu je najveća prednost. Također, velika prednost je i cijena koja je neusporedivo manja u odnosu na komercijalne alate. Moguće je ekstrahirati podatke s uređaja na kojima nedostaje SIM kartica kao i s uređaja kojima nedostaje baterija. Najveći nedostatak ove metode je što ona nije *forensically sound* i nije bila zamišljena kao sredstvo za forenzičku analizu, a to može

rezultirati ugrožavanjem integriteta podataka. Metoda je invazivna i može izmijeniti podatke, a to je veliki nedostatak. Niska cijena može predstavljati i problem, jer je lako dostupna običnim osobama koje ga mogu nabaviti i koristiti ga u protuzakonite svrhe. Problem predstavlja i to što je za pokretanje ekstrakcije često potrebno ponovno pokretanje mobilnog uređaja što može uzrokovati aktiviranje mehanizama za provjeru autentičnosti i sprječavanje daljnje analize, [49].

Slika 5: Prikaz ekstrakcije mobilnog uređaja korištenjem Flasher Box-a, [50]

3.2.2.2. Ekstrakcija podataka mobilnih uređaja s Cloud pohrane

Ekstrakcija podataka iz *Cloud*-a jedna je od manje zastupljenih metoda ekstrakcije, no vremenom će postati sve značajnija jer se svakodnevno pohranjuje sve više podataka na *Cloud* pohranu. Mobilni *Cloud*, odnosno mobilno računalstvo u oblaku je kombinacija mobilnih mreža i računalstva u oblaku koja omogućuje pohranjivanje korisničkih aplikacija i podataka na neko udaljeno mjesto, a ne na memoriju uređaja. Ti podaci mogu biti pohranjeni na različitim geografskim lokacija što može predstavljati veliki problem za forenzičke istražitelje tijekom istrage. Postoji nekoliko čimbenika u okruženju računalstva u oblaku koji predstavljaju izazov forenzičkim ispitivačima u odabiru tehnika i alata za provođenje ekstrakcije. Uz to, oporavak korisničkih podataka pohranjenih u oblaku može biti problematičan zbog zakona i propisa koji nisu dobro definirani u ovome trenutku. U današnje vrijeme forenzički ispitivači moraju voditi računa o ovoj vrsti pohrane i podacima koji se u njoj nalaze jer u nekim slučajevima ti podaci mogu biti krucijalni za istragu, [18]. Teško je identificirati, prikupiti, sačuvati i integrirati digitalne dokaze s *Cloud* pohrane, a razlog tomu su brojne njegove karakteristike, kao što su: virtualizacija, skalabilnost, distribuirane mreže, itd, [51].

Vrlo često se sigurnosna kopija mobilnog uređaja pohranjuje upravo na *Cloud*, što također predstavlja izazov forenzičkom ispitivaču. Gotovo sve društvene mreže pohranjuju svoje podatke odnosno sigurnosne kopije u računalstvo u oblaku, neki od njih su: *Dropbox,*

Facebook, Twitter, Instagram, Google Drive, itd. Poznato je da su društvene mreže u velikoj većini slučajeva dobar izvor digitalnih dokaza kojima se mogu riješiti razne istrage, stoga forenzički istražitelji moraju posvetiti dosta pažnje ovom potencijalnom izvoru digitalnih dokaza, [52].

Prednost ove vrste pohrane za korisnike je sigurnost i tajnost lokacije podataka te gotovo neograničen memorijski prostor. Što se tiče ekstrakcije podataka, prednost predstavlja mogućnost pristupanja i ekstrakcije podataka bez poznavanja lokacije tih podataka, a sama ekstrakcija je nedestruktivna i neinvazivna. Ekstrakcija podataka iz *Cloud*-a predstavlja veliki izazov i ima mnogo ograničenja. Jedan od problema za forenzičkog istražitelja je virtualizirano okruženje u kojemu se na puno teži način dolazi do podataka. Također, problem predstavlja nedostatak komercijalnih alata usmjerenih ekstrakciji podataka s *Cloud*-a. Podaci koji su pohranjeni u *Cloud*-u ne moraju biti blizu jedni drugima što može predstavljati problem i odužiti forenzičku istragu. Dokazivanje vlasništva ekstrahiranih podataka također je jedan od problema s kojima se susreću forenzički istražitelji, a razlog tomu je neravnomjerni postupak provjere autentičnosti i autorizacije na uređaju i u *Cloud*-u, [53].

4. Karakteristike forenzičkog alata SPF Pro

Alati mobilne forenzike moraju biti u stalnom razvoju kako bi pratili trendove novih mobilnih uređaja te kako bi se osigurao prikladan način ekstrahiranja podataka s različitih mobilnih uređaja, a za ekstrakciju se uglavnom koriste kablovi, infracrvene veze, *Bluetooth* tehnologija ili JTAG. Većina forenzičkih alata rade na jednakom principu, a to je da šalju naredbe prema mobilnom uređaju i bilježe odgovore koji sadrže podatke pohranjene u memoriji mobilnog uređaja. Količina povratnih informacija, odnosno podataka koje uređaj šalje prema forenzičkom alatu ovise o vrsti veze te modelu mobilnog uređaja, [17]. U ovom poglavlju prikazat će se forenzički alat SPF Pro kod kojeg također količina ekstrahiranih podataka ovisi o modelu mobilnog uređaja te operativnog sustava na kojem radi.

4.1. Svrha alata mobilne forenzike

Osnovna svrha alata mobilne forenzike je pronalaženje dokaza te određivanje je li osumnjičena osoba počinila kriminalnu radnju ili nije. Forenzički alati moraju biti validirani kako bi bili prihvatljivi na sudu te u tu svrhu moraju ispunjavati određene zakonske uvjete, [54]. Alati mobilne forenzike predviđeni su za pomoć službenicima osiguranja, policijskim i pravnim istražiteljima u postupcima identifikacije, prikupljanja, očuvanja te ispitivanja podataka koji su povezani s neprimjerenim i nezakonitim aktivnostima, poput zloupotrebe e-pošte i Interneta, financijskog lošeg upravljanja, neovlaštenog otkrivanja korporativnih podataka, krađa intelektualnog vlasništva, itd. Tri osnovne funkcije mobilnih forenzičkih alata su stjecanje, prikupljanje i očuvanje. Odabir odgovarajućeg forenzičkog alata za određeni slučaj mora poštivati sljedeće kriterije: povezanost sa zakonom, sposobnost očuvanja prikupljenih podataka, integracija te mogućnost upravljanja predmetima, [55]. Sustavi forenzičkih alata komuniciraju s operativnim sustavima mobilnih uređaja kako bi mogli ekstrahirati podatke. Ti sustavi imaju ograničenja u vidu informacija koje se mogu ekstrahirati jer postoji mogućnost da će biti dostupne samo informacije vezane za operativni sustav. Ta ograničenja mogu dovesti do toga da se potencijalno relevantne informacije za forenzičku istragu možda neće moći ekstrahirati, [17].

4.1.1. Zahtjevi alata mobilne forenzike

Alati mobilne forenzike moraju imati određene smjernice i zahtjeve kako bi bili pravovaljani. Ako određeni forenzički alati ne ispunjavaju te zahtjeve, neće biti prihvatljivi na sudu te podaci koje su ekstrahirali neće se moći uzeti u obzir. U nastavku se nalaze zahtjevi koje mobilni forenzički alati moraju zadovoljiti.

- **Upotrebljivost** – Da bi se riješio problem složenosti (podatke u osnovnom formatu je teško analizirati) alati moraju dati podatke na sloju apstrakcije i formatu koji potencijalno mogu olakšati posao forenzičkom istražitelju. U najmanju ruku, forenzički istražitelj mora imati pristup slojevima apstrakcije koji su definirani kao granični slojevi.
- **Opsežnost** – Da bi se utvrdili i identificirali dokazi, forenzički istražitelji moraju imati pristup svim izlaznim podacima na zadanom sloju apstrakcije. Svaki dio memorije mobilnog uređaja sadrži zapise koji potencijalno mogu sadržavati dokaze o određenom kaznenom djelu, stoga je potrebno da forenzički alati provode opsežne forenzičke istrage.
- **Točnost** - Za rješavanje problema s pogreškama (slojevi apstrakcije uvode pogreške u završne ekstrahirane podatke) mobilni forenzički alati moraju osigurati točnost izlaznih podataka te se izračunavaju pogreške kako bi se podaci mogli pravilno interpretirati.
- **Determinističnost** – Kako bi se osigurala točnost i povjerljivost alata, uvijek se mora moći provjeriti izlazni rezultat. To se može učiniti ručno ili korištenjem drugog i neovisnog forenzičkog alata. Stoga se mora omogućiti pristup ulazima i izlazima svakog sloja kako bi se izlazni podaci mogli provjeriti.
- ***Read-Only* –** Ovaj zahtjev nije nužan, no preporučuje se. Kako priroda digitalnih medija omogućuje jednostavno stvaranje kopija podataka, kopije se mogu napraviti prije korištenja alata. Za provjeru rezultata što je ujedno i uvjet ovog zahtjeva, potrebna je kopija unosa, [56].

4.1.2. Osnovna podjela alata mobilne forenzike

Alati mobilne forenzike mogu se klasificirati prema mnogo kriterija, a neki od njih su: podržane ekstrakcije, količina podataka koje mogu ekstrahirati, jednostavnost uporabe, mogućnost zaobilaženja zaporki te brojni drugi.

Osnovna podjela alata mobilne forenzike je:

- **Hardverski alati** - Osmišljeni su prije svega za ispitivanje uređaja za pohranu, a cilj im je da sumnjivi uređaji ostanu nepromijenjeni kako bi se očuvala cjelovitost dokaza. Kao što im samo ime kaže, hardverski alati podrazumijevaju uređaj ili neku drugu vanjsku jedinicu kojom se vrši ekstrakcija s mobilnih uređaja. Također, podrazumijevaju korištenje velikog broja kablova za povezivanje s mobilnim uređajem. U većini slučajeva, ekstrakcija korištenjem hardverskih alata traje duže, no ona je sadržajna i cjelovita.
- **Softverski alati** – Ti alati su u obliku aplikacije, a oni su uglavnom višenamjenski i mogu obavljati različite zadatke u jednoj aplikaciji. Određeni softverski alati mogu istovremeno obrađivati više uređaja ili upravljati različitim operativnim sustavima. Gotovo svi softverski alati mogu analizirati digitalne dokaze koje su ekstrahirali s

mobilnih uređaja, [57]. Softverski alati moraju biti pokrenuti na određenom hardveru te je u većini slučajeva njihova ekstrakcija podataka nešto slabija od hardverskih forenzičkih alata, [58].

4.2. Ključne značajke alata SPF Pro

SPF Pro (engl. *Smartphone Forensic Professional*) softverski je forenzički alat kineske tvrtke SalvationDATA. SalvationDATA je vodeći kineski pružatelj integriranih rješenja digitalne forenzike, oporavka podataka, sigurnosti podataka te pronalazaka digitalnih dokaza, [59]. SPF Pro je *forensically sound* forenzički alat koji je namijenjen za ekstrakciju, otkrivanje, analizu te trijažne postupke nad mobilnim uređajima. Predstavlja novu generaciju forenzičkih alata tvrtke SalvationDATA i snažna je integrirana platforma za digitalne istrage. Omogućuje istražiteljima da lako i učinkovito pregledaju i utvrde relevantne informacije s mobilnih uređaja, kako na terenu tako i u laboratoriju, a također im pomaže da se oporave i prikupe kritični forenzički dokazi iz brojnih zapisa i zaključanih pametnih mobilnih uređaja pomoću funkcija s više zadataka i inteligentne analize. Također, SPF Pro može automatski odabrati najbolje rješenje za ekstrakciju podataka. Ovaj alat usmjeren je prema kineskim mobilnim uređajima te za njih nudi najviše mogućnosti ekstrakcije podataka.

Kao što je navedeno SPF Pro je usmjeren kineskim mobilnim uređajima, no podržava i ostale uređaje. Podržani brendovi su: iPhone, Samsung, Huawei, OPPO, VIVO, Mi, HTC, Blackberry, Nokia, Motorola, NEC, Dopod, Sony Ericsson, LG, ZTE, Lenovo, MEIZU, Coolpad te brojni drugi kineski brendovi. SPF Pro također podržava i brojne operativne sustave, a to su: Android, iOS, Firefox OS, Yun OS, Blackberry, Windows Mobile, Ubuntu, MTK, Speadtrum te također brojne druge kineske operativne sustave za pametne mobilne uređaje, [60].

Velika prednost forenzičkog alata SPF Pro je automatsko otkrivanje proizvođača i modela pametnog mobilnog uređaja te preporuke za izbor načina ekstrakcije podataka za otkriveni mobilni uređaj. SPF Pro ima mogućnost obavljanja više zadataka u isto vrijeme, a maksimalni broj zadataka koji se mogu obavljati u isto vrijeme je osam. Sadrži mogućnost inteligentne analize koja automatski upozorava korisnika kada se otkriju osjetljivi podaci. Te stavke za analizu uključuju ključne riječi, aplikacije, URL (engl. *Uniform Resource Locator*) –ove, MD5 *hash*, itd, [61].

4.3. Rad u alatu SPF Pro

Kao i u svakom drugom forenzičkom alatu ili aplikaciji na računalu, potrebno je upisati korisničko ime i lozinku za pristup sustavu. U slučaju alata SPF Pro prethodno je potrebno izvršiti aktivaciju alata upisivanjem ključa koji se dobio od tvrtke SalvationDATA.

Nakon prijave u sustav, otvara se glavno sučelje alata. To sučelje nudi glavne mogućnosti alata te svaka ekstrakcija ili bilo koja druga aktivnost podrazumijeva aktivnost na ovome sučelju.

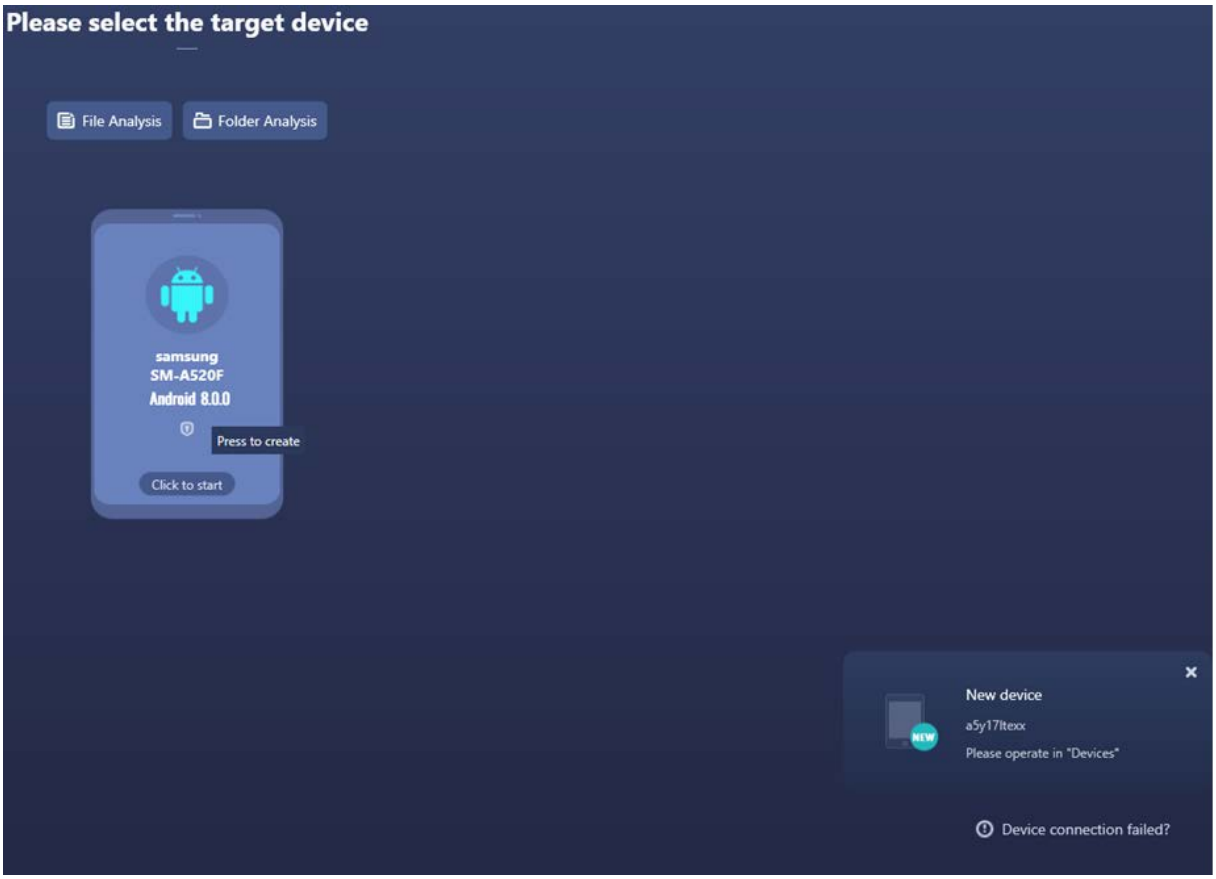
Slika 6: Sučelje za upravljanje sustavom

Na slici 6 prikazano je osnovno sučelje alata SPF Pro putem kojega se poduzimaju svi osnovni koraci. Svaka aktivnost koja se nalazi na slici bit će opisana u nastavku. Slika 6 podijeljena je u pet osnovnih dijelova koji naznačuju glavne radnje na sučelju za upravljanje sustavom.

1. Dio naznačen brojem 1 označava tipku kojom se pokreće izrada novog slučaja, a sam postupak je jednostavan i lako razumljiv svakoj osobi koja poznaje rad na računalu. U tu svrhu upisuju se i određuju osnovni elementi slučaja, kao što su: naziv slučaja, vrsta slučaja, ime i prezime forenzičkog istražitelja, a neki elementi kao što je datum i vrijeme sami se generiraju.
2. Element koji je naznačen s 2 prikazuje tipku kojom se otvaraju postojeći slučajevi, odnosno postojeće ekstrakcije podataka što je također vrlo lako razumljivo.
3. Treći dio prikazuje nedavne slučajeve, odnosno obrade uređaja. Prikazan je naziv slučaja kojeg je korisnik alata SPF Pro samostalno unio te datum zadnjeg korištenja tog slučaja.
4. Dio naznačen s 4 označava alate unutar alata SPF Pro. Njih ima mnogo i bit će objašnjeni u nastavku rada.
5. Peti dio prikazuje osnovne funkcije za upravljanje alatom SPF Pro.

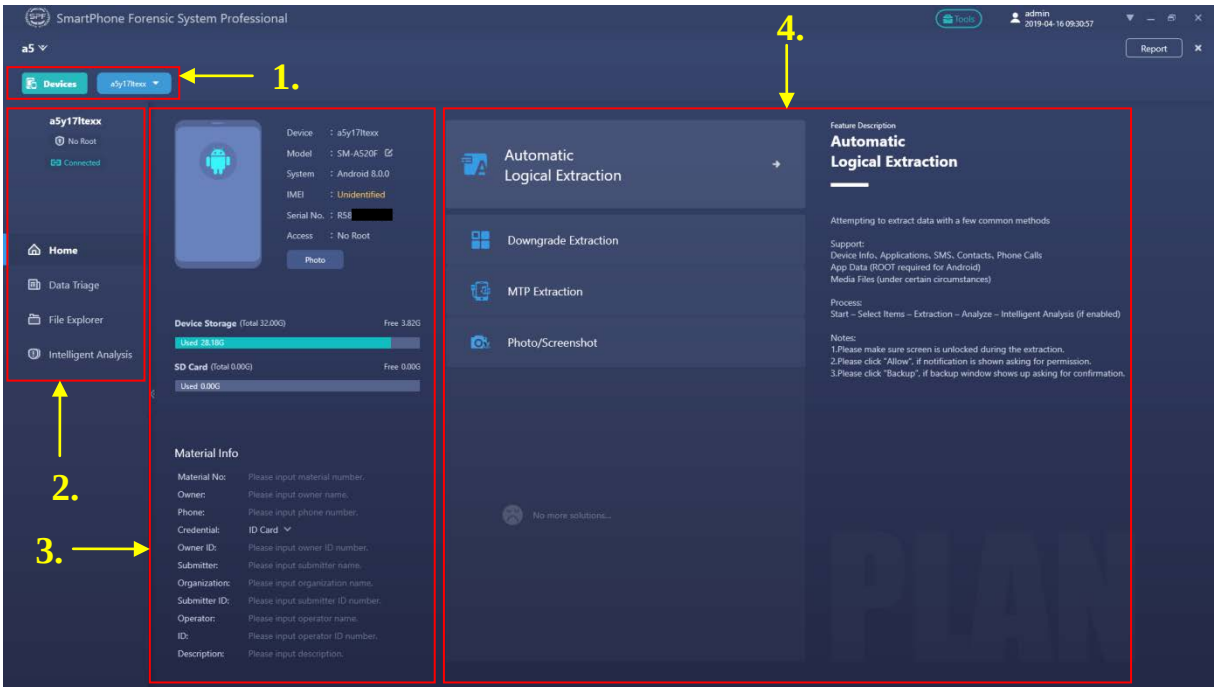
Vrlo važan element u radu alata SPF Pro je prepoznavanje povezanog uređaja. SPF Pro to radi na učinkovit i brz način te se tijekom izrade diplomskog rada nisu pojavljivale

poteškoće u prepoznavanju mobilnog uređaja. Sljedeća slika prikazuje način na koji SPF Pro prepoznaje povezani mobilni uređaj.



Slika 7: Odabir uređaja za ekstrakciju podataka

Nakon što se mobilni uređaj poveže na računalo svojim kabelom, najprije će se u donjem desnom kutu prikazati da je uređaj povezan, a zatim će biti raspoloživ za njegovo odabiranje za ekstrakciju podataka. Na slici 7 vidljivo je da se uz proizvođača i model uređaja nalazi informacija o verziji operativnog sustava. Potrebno je odabrati prepoznati uređaj kako bi se nastavio postupak koji vodi prema ekstrakciji podataka.



Slika 8: Informacije o mobilnom uređaju te mogućnosti ekstrakcije podataka

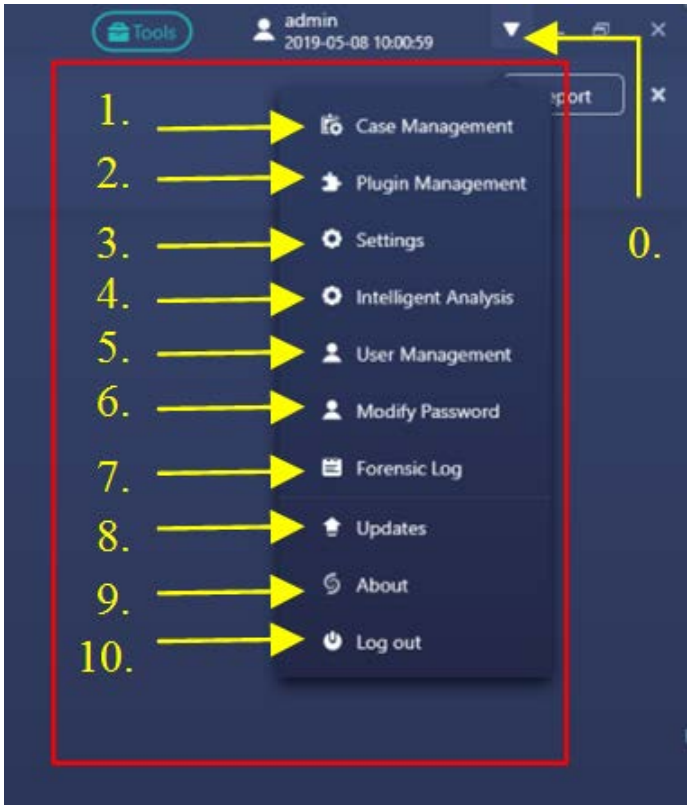
Slika 8 predstavlja glavno sučelje za ekstrakciju podataka u kojemu je moguće vidjeti i odabrati najvažnije funkcije. Slika je podijeljena u četiri elementa koja razdjeljuju sučelje u četiri osnovne jedinice, a svaka od njih je opisana u nastavku:

1. Element naznačen kao 1 prikazuje uređaje koji su otvoreni kao zasebni slučaj, a uređaji se odabiru na slici 7. Na slici 8 radi se o jednom otvorenom slučaju, odnosno jednom uređaju koji se obrađuje te je moguće vidjeti naziv uređaja.
2. Unutar elementa naznačenog s 2 nalazi se naziv uređaja, a u ovom otvorenom slučaju radi se o uređaju Samsung Galaxy A5 što je moguće prepoznati iz njegovog naziva. Prikazuje se informacija o *Root* statusu uređaja, odnosno je li *Root* status omogućen ili nije. U ovom slučaju mobilni uređaj Samsung Galaxy A5 nije *Root*-an. Također prikazana je i informacija o tome je li uređaj povezan s računalom ili nije, ali u svakom odvojenom slučaju uređaj mora biti povezan jer se inače ne bi moglo upravljati njime kroz alat SPF Pro. Prikazane su i mogućnosti pregledavanja uređaja, koje uključuju trijažne postupke, pregledavanje datoteka u uređaju te inteligentnu analizu, no to će biti detaljnije opisano u poglavlju 6.
3. Treći element prikazuje osnovne informacije o mobilnom uređaju. Kao i u prethodna dva pravokutnika i ovaj prikazuje ime uređaja. Osim imena uređaja, moguće je vidjeti i model uređaja, a u ovom slučaju radi se o SM – 520F, odnosno Samsung Galaxy A5. Prikazana je i verzija operativnog sustava na kojem on radi, kao i njegovi osnovni podaci (IMEI, serijski broj) te *Root* status. Uz to prikazuje se memorija uređaja te koliko je ona zauzeta, kao i memorija SD kartice, ako je mobilni uređaj sadrži.
4. Element naznačen kao 4 prikazuje mogućnosti ekstrakcije za povezani mobilni uređaj. Broj odnosno raznolikost mogućnosti ekstrakcije podataka može se razlikovati zbog mnogo faktora. Jedan od njih je *root* pristup, model uređaja, model operativnog

sustava, i sl. Kineski mobilni uređaji imaju najviše mogućnosti ekstrakcije podataka, no to je i logično jer je kreator ovog forenzičkog alata kineska tvrtka.

4.3.1. Osnovne funkcije upravljanja alatom SPF Pro

Sljedeća slika daje prikaz osnovnih mogućnosti upravljanja alatom SPF Pro. Većina aplikativnih rješenja te softverskih forenzičkih alata ima slične mogućnosti.



Slika 9: Osnovne funkcije upravljanja alatom SPF Pro

Kako bi se otvorio skočni prozor u kojemu se nalaze osnovne funkcije upravljanja alatom SPF Pro potrebno je kliknuti na dio koji je označen kao 0. Padajući izbornik alata nalazi se unutar crvenog kvadrata, a redni brojevi označavaju pojedine mogućnosti kojima se upravlja alatom. Svrha svake mogućnosti opisana je u nastavku:

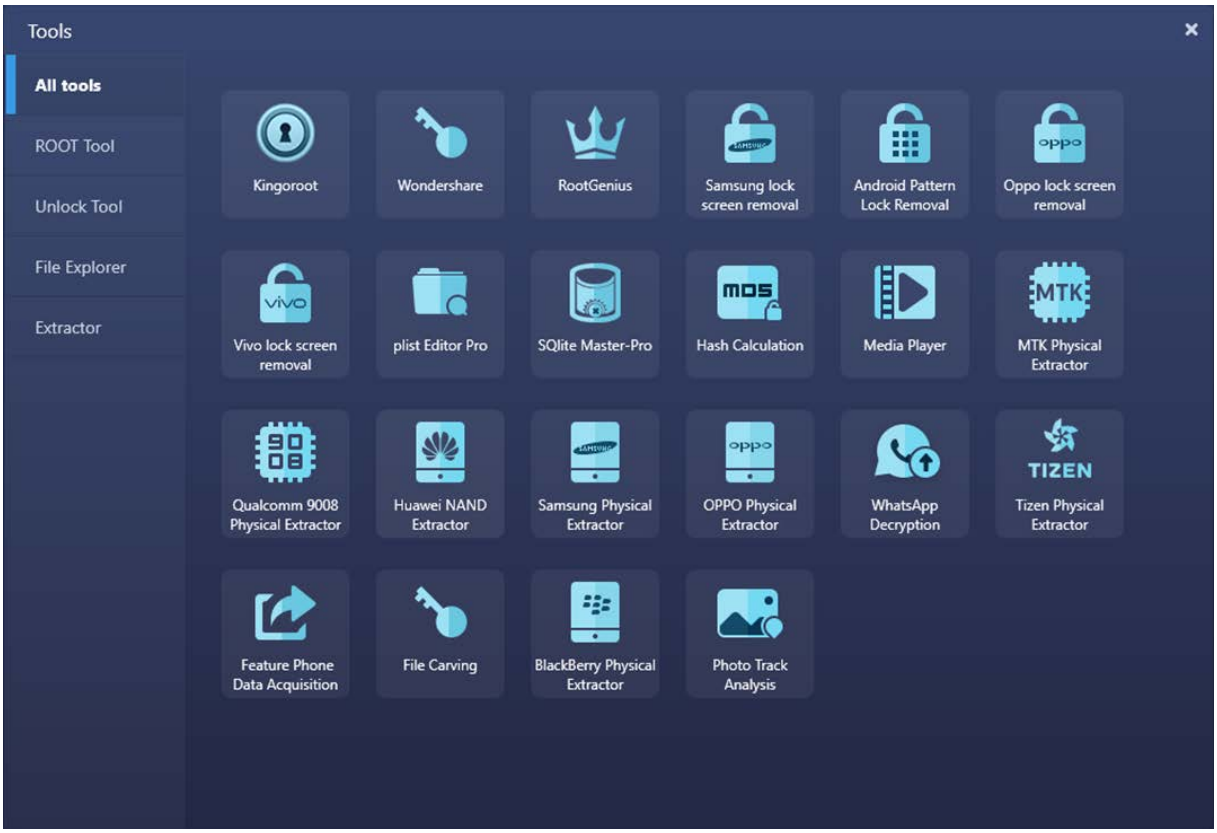
1. **Upravljanje slučajevima** (engl. *Case Management*) – Omogućuje jednostavno upravljanje slučajevima, odnosno otvaranje, brisanje ili pretraživanje pojedinog pohranjenog slučaja prema vremenu ili ključnim riječima.
2. **Upravljanje ekstrahiranim podacima** (engl. *Plugin Management*) – Omogućuje pregledavanje svih dodataka instaliranih u sustavima. Drugim riječima, omogućuje prikaz izvora podataka koji su ekstrahirani, kao što je to zapisnik poziva te se prikazuju njegove pojedinosti, kao što je operativni sustav iz kojeg su podaci

ekstrahirani, metoda ekstrakcije, naziv tog izvora podataka u pojedinom mobilnom uređaju, i sl.

3. **Postavke** (engl. *Settings*) – Kao i u većini aplikacija i programa, u postavkama alata SPF Pro odabire se jezik, predefinirana datoteka u koju se pohranjuju slučajevi te brojne druge osnovne postavke.
4. **Pametno pretraživanje** (engl. *Intelligent Analysis*) – Omogućuje ili onemogućuje provedbu pametnog pretraživanja. Kad je opcija omogućena, SPF Pro će inteligentno nadgledati i upozoriti korisnika alata na osjetljive podatke. Također moguće je postaviti ključne riječi koje će se pretražiti prilikom analize, a moguće je i omogućiti ili onemogućiti pretragu po sljedećim kriterijima: pornografija, droga i nasilje.
5. **Izmjena lozinke** (engl. *Modify Password*) – Omogućuje promjenu lozinke korisnika alata na vrlo jednostavan način, kao što je to slučaj kod većine programa ili aplikacija gdje postoji korisnik, odnosno korisnički račun.
6. **Upravljanje korisnicima** (engl. *User Management*) – Omogućuje dodavanje novog korisnika, brisanje postojećih te izmjenu imena korisnika, organizacije kojoj pripada, kontakta, i sl.
7. **Forenzički zapisi** (engl. *Forensic Log*) – Prikazuje osnovne zapise o ekstrakcijama, odnosno sve operacije koje su se događale u alatu SPF Pro. Tako na primjer, prikazuje operaciju otvaranja novog slučaja te za tu i svaku drugu operaciju navodi korisnika koji ju je izveo, datum izvedbe i snimku zaslona ako ona postoji,
8. **Nadogradnje** (engl. *Updates*) – Omogućuje pregledavanje postojeće verzije alata te postoji li novija verzija na koju je moguće nadograditi alat SPF Pro.
9. **O alatu** (engl. *About*) – Omogućuje pregledavanje osnovnih informacija o alatu. Prikazana je verzija alata, kao i trajanje licence koja omogućuje korištenje. Također, navedene su osnovne informacije o tvrtki SalvationDATA, kao što su adresa, poštanski broj, broj telefona, *web* stranica, itd.
10. **Odjava** (engl. *Log Out*) – Jednostavna opcija kojom se trenutni korisnik odjavljuje te je za njegovo ponovno korištenje potrebno unijeti korisničko ime i lozinku.

4.3.2. Dodatni alati unutar alata SPF Pro

Veliku prednost alata SPF Pro čine brojni dodatni alati koji su instalirani, odnosno smješteni unutar samog alata SPF Pro. Ti alati mogu pomoći korisnicima alata u ekstrakciji podataka mobilnih uređaja, pripremanju uređaja za ekstrakciju te brojne druge funkcije. Ti dodatni alati štede vrijeme korisnika alata, jer uz njih nije potrebno dodatno pretraživanje alata na Internetu. Sljedeća slika prikazuje dodatne alate svrstane u četiri kategorije.



Slika 10: Alati za ostvarivanje *Root* pristupa na mobilnim uređajima

Slika 10 prikazuje dodatne alate unutar softverskog forenzičkog alata SPF Pro. Oni su svrstani u četiri skupine, a to su:

- Alati za *Root*-anje uređaja
- Alati za otključavanje uređaja
- Alati za pretraživanje datoteka
- Alati za ekstrakciju

Alati za Root-anje uređaja usmjereni su ostvarivanju punog pristupa mobilnom uređaju. *Root*-anje predstavlja proces kojim se omogućuje pametnim mobilnim uređajima, tabletima i ostalim uređajima temeljenim na Unix operativnom sustavu puni pristup operativnom sustavu što omogućuje brisanje i modificiranje sistemskih datoteka. Moguće je protumačiti te pune ovlasti na mobilnom uređaju kao administrativne ovlasti na računalu, [62]. Na *Root*-anim uređajima moguće je zaobići bilo kakva ograničenja postavljena od strane proizvođača ili pružatelja mobilnih usluga, brisati aplikacije koje se inače ne bi mogle obrisati, ručno dijeliti dopuštenja aplikacijama i sl. Za iPhone i ostale iOS uređaje postupak omogućavanja potpunog pristupa operativnom sustavu naziva se *jailbreak*. Uz prethodno navedene pozitivne strane *Root*-anja, postoje i negativne strane, a one su: mogući gubitak garancije uređaja, rušenje sustava mobilnog uređaja, gubitak trenutnih podataka i sl. Također, važno je naglasiti da ne postoji standardni postupak kojim se ostvaruje *Root* pristup na mobilnom uređaju te je on različit gotovo za svaki uređaj, [63].

Alat SPF Pro sadrži tri alata za *Root*-anje mobilnih uređaja. To su alati *Kingoroot, Wondershare* i *RootGenius*. Sva 3 alata rade na sličan način, a to je prepoznavanje i prikaz uređaja na zaslonu nakon povezivanja s računalom. Sva 3 alata su vrlo jednostavna i smatra ih se alatima za *One-Click-Root,* odnosno *Root*-anje jednim klikom miša. Sva 3 alata su isprobana na različitim uređajima i moguće je zaključiti da ne rade na način za koji se smatra da rade jer je *Root* status ostvaren samo na jednom uređaju, a to je Samsung Galaxy S3 Mini korištenjem alata *Kingoroot*.

Alati za otključavanje uređaja usmjereni su uklanjanju odnosno otključavanju zaslona mobilnog uređaja. Dostupna su četiri različita alata te su usmjerena točno određenim uređajima, a to su: Samsung uređaji, Android uređaji, Oppo uređaji te Vivo uređaji. Od četiri navedena alata, dva su isprobana, a to *su Samsung lock screen removal i Android Pattern Lock Removal* te niti jedan od njih ne radi prema očekivanjima, odnosno niti jedan nije otključao tj. uklonio lozinku/uzorak s mobilnih uređaja. Oba alata su prikazala da je postupak otključavanja izvršen, no na uređajima se nije događala nikakva promjena. U tu svrhu koristili su se uređaji: Samsung Galaxy A5, HTC Desire 610, Samsung Galaxy A8, Samsung Galaxy S4 i Samsung Galaxy S3 Mini. *Oppo lock screen removal* i *Vivo lock screen removal* nisu isprobani jer za potrebe diplomskog rada nisu bile dostupne takve vrste mobilnih uređaja.

Alati za pretraživanje datoteka usmjereni su pretraživanju različitih datoteka korištenjem brojnih naredbi. SPF Pro omogućuje pretraživanje datoteka sljedećim alatima: *plist Editor Pro, SQL Master Pro, Hash Calculation* i alatom *Media Player*.

- ***plist Editor Pro*** - usmjeren je pretraživanju plist-a. Plist (engl. *Property List*) datoteke predstavljaju datoteke s postavkama, poznate i kao „datoteke svojstava“, koju koriste macOS aplikacije. Sadrže svojstva i postavke konfiguracije za različite programe. Plist datoteke formatiraju se u XML-u (engl. *Extensible Markup Language*) i uglavnom se upotrebljavaju na iOS platformama. One se mogu spremati u binarnom ili tekstualnom formatu, a često se koriste za pohranjivanje korisničkih postavki i pohranu podataka o aplikacijama, [64]. Alat plist Editor Pro koji se nalazi u sklopu alata SPF Pro omogućuje pregledavanje i uređivanje tih XML zapisa koji prikazuju postavke konfiguracije za iOS uređaje. Ti zapisi mogu biti vrlo korisni za povezivanje postavki aplikacija i uređaja te ostalih ekstrahiranih podataka kako bi se uspješno rekonstruirali određeni događaji i riješili slučajevi koji se istražuju.
- ***SQL Master Pro*** - SQL (engl. *Structured Query Language*) je standardni jezik za pohranu, manipuliranje i dohvaćanje podataka u bazama podataka. Od 1987. godine SQL je međunarodni standard prema ISO-u, [65]. *SQL Master Pro* unutar alata SPF Pro služi za pretraživanje baza podataka na mobilnim uređajima ili na *Cloud* pohrani postavljanjem upita. Najčešći upiti odnose se na datum, vrijeme, vremenske oznake te intervale. Omogućava učinkovit pregled baza podataka, a uglavnom se koristi nakon provođenja same ekstrakcije te ako rezultat ekstrakcije ne daje dovoljno podataka o strukturi mobilnih uređaja te baza podataka.
- ***Hash Calculation*** – Predstavlja kalkulator koji se odnosi na MD5, tehnički nazvan MD5 algoritam za razbijanje poruka, a njegova osnovna funkcija je izračunavanje vrijednosti i provjera da datoteka nije promijenjena. Kalkulator to čini izradom

kontrolnog zbroja za oba skupa, a zatim uspoređivanjem kontrolnih zbrojeva kako bi se potvrdilo da su isti. Ima određene nedostatke, pa nije koristan za napredne aplikacije za šifriranje, ali je potpuno prihvatljivo da se koristi za standardne provjere datoteka, [66]. Hash Calculation u sklopu alata SPF Pro radi na način kao i svi drugi kalkulatori iste svrhe. Potrebno je unijeti MD5 hash vrijednost određene datoteke, a kalkulator će izračunati je li ta datoteka promijenjena ili nije, odnosno rezultat mora biti jednak unesenoj vrijednosti.

- ***Media Player*** – Ima istu svrhu kao i bilo koji drugi preglednik videozapisa, slika te ostalih medijskih zapisa. Putem njega se mogu pregledavati videozapisi, slike te zvukovi koji su ekstrahirani iz mobilnih uređaja

Alati za ekstrakciju predstavljaju pomoć u provođenju ekstrakcije podataka posebnih mobilnih uređaja. Odnose se na točno određene mobilne uređaje ili točno određenu skupinu podataka, a oni su: *MTK Physical Extractor*, *Qualcomm 9008 Physical Extractor*, *Huawei NAND Extractor*, *Samsung Physical Extractor*, *Oppo Physical Extractor*,*Whatsapp Decryption*, *Tizien Physical Extractor*, *Feature Phone Data Acquisition*, *File Carving*, *BlackBerry Physical Extractor* i *Photo Track Analysis*. Od navedenih alata testirana su dva, a oni ne rade na zadovoljavajuć način. Prvi od tih alata je *Samsung Physical Extractor* koji pruža mogućnost ekstrakcije samo za dva mobilna uređaja koji nisu bili dostupni za izradu diplomskog rada. Drugi je *WhatsApp Decryption* koji tvrtka SalvationDATA predstavlja kao moćno sredstvo ekstrakcije poruka i ostalih podataka *WhatsApp* aplikacije. Testiranje ovog alata izvršeno je na četiri mobilna uređaja (Samsung Galaxy S3 Mini, Samsung Galaxy A5, HTC Desire 610 i iPhone4), a on nije ekstrahirao nikakve podatke ni za jedan mobilni uređaj. Ostali alati su pregledani i neki od njih ne rade na način na koji bi trebali (npr. *Photo Track Analysis*), a provođenje ekstrakcije tim alatima nije bilo moguće zbog nedostatka mobilnih uređaja za potrebe diplomskog rada.

4.4. Usporedni prikaz mogućnosti alata SPF Pro u odnosu na druge alate iste namjene

Softverski alat SPF Pro predstavlja dobro rješenje za jednostavnu provedbu forenzičke analize nad mobilnim uređajima. Postoje brojni alati koji se koriste u istu svrhu kao i SPF Pro, no svaki od njih ima određene prednosti i nedostatke u odnosu na SPF Pro. Sljedeća tablica daje uvid u osnovne mogućnosti alata SPF Pro u odnosu na druge alate iste namjene. Tablica je izrađena na temelju alata SPF Pro i njegovih mogućnosti, a usporedba se odnosi na ostale alate te njihovu mogućnost zadovoljavanja istih mogućnosti koje sadrži softverski alat SPF Pro.

Tablica 1: Usporedba alata SPF Pro u odnosu na druge alate iste namjene
Izvor: [67]

	SPF PRO	UFED	XRY	AXIOM	Oxygen	BlackBag	MOBILedit	FINALMobile	ElcomSoft
Automatska preporuka za metodu ekstrakcije	√	√						√	
Multi-tasking	√	√	√				√		√
Inteligentna analiza	√	√	√	√	√	√	√		
Podrška za kinesku *Chipset* platformu	MTK, Symbian Spreadtrum CoolSand Skyoworks INFENON,ADI AGERE,Mstar TI, ADI, SI, AnyKa, CDMA, AD6905	MTK Symbian Spreadtrum INFENON CDMA	MTK SpreadTrum Coolsand Infineon	MTK	MTK Spreadtrum				
Fizička ekstrakcija za MTK i Qualcomm	√	√	√		√				
Fragmentirano obnavljanje podataka	√	√	√		√			√	
Nastavak prekida ekstrakcije	√	√				√			
WhatsApp dešifriranje	√	√							√
Ekstrakcija datotečnog sustava	√	√	√	√	√		√		√
Zbirka dokaza u stvarnom vremenu	√	√	√	√	√	√			

U tablici 1 vidljivo je da su mogućnosti usmjerene kineskim mobilnim uređajima, a razlog tomu je što je tablica izrađena prema mogućnostima alata SPF Pro. Vidljivo je da je UFED Touch 2 jedini alat koji se s kineskim uređajima može nositi na jednak način kao i SPF Pro. To ne čudi jer je UFED Touch 2 prema brojnim izvorima trenutačno optimalan alat za forenzičku analizu mobilnih uređaja. Ostali alati omogućavaju neke funkcionalnosti, ali ne sve kao što to mogu SPF Pro i UFED Touch 2 što je jasno prikazano u tablici.

5. Provedba forenzičke analize korištenjem alata SPF Pro

Kao što je navedeno u drugom poglavlju, digitalna forenzička analiza predstavlja proces otkrivanja i tumačenja elektroničkih podataka koji se nalaze na određenom digitalnom mediju. Za potrebe ovog diplomskog rada, forenzička analiza se provodi nad nekoliko mobilnih uređaja što će biti detaljnije opisano u nastavku. Osnovni cilj tijekom provedbe forenzičke analize je očuvanje podataka, odnosno onemogućavanje njihove promjene. Također, cijeli postupak forenzičke analize mora biti dobro dokumentiran.

Provođenje forenzičke analize, odnosno ekstrakcije i pronalaska podataka na mobilnim uređajima korištenjem softverskog alata SPF Pro ne predstavlja velik napor. Razlog tomu su brojne mogućnosti koje sam alat pruža. Neke od mogućnosti uključuju automatsko i samostalno prepoznavanje povezanih uređaja te automatsko predlaganje metoda ekstrakcije podataka. Tijekom provedbe forenzičke analize korištenjem alata SPF Pro potrebno je dobro pratiti korake i što se točno traži.

Za potrebe diplomskog rada korišteni su sljedeći mobilni uređaji:

- Samsung Galaxy S3 Mini
- Samsung Galaxy A5
- HTC Desire 610
- iPhone 4

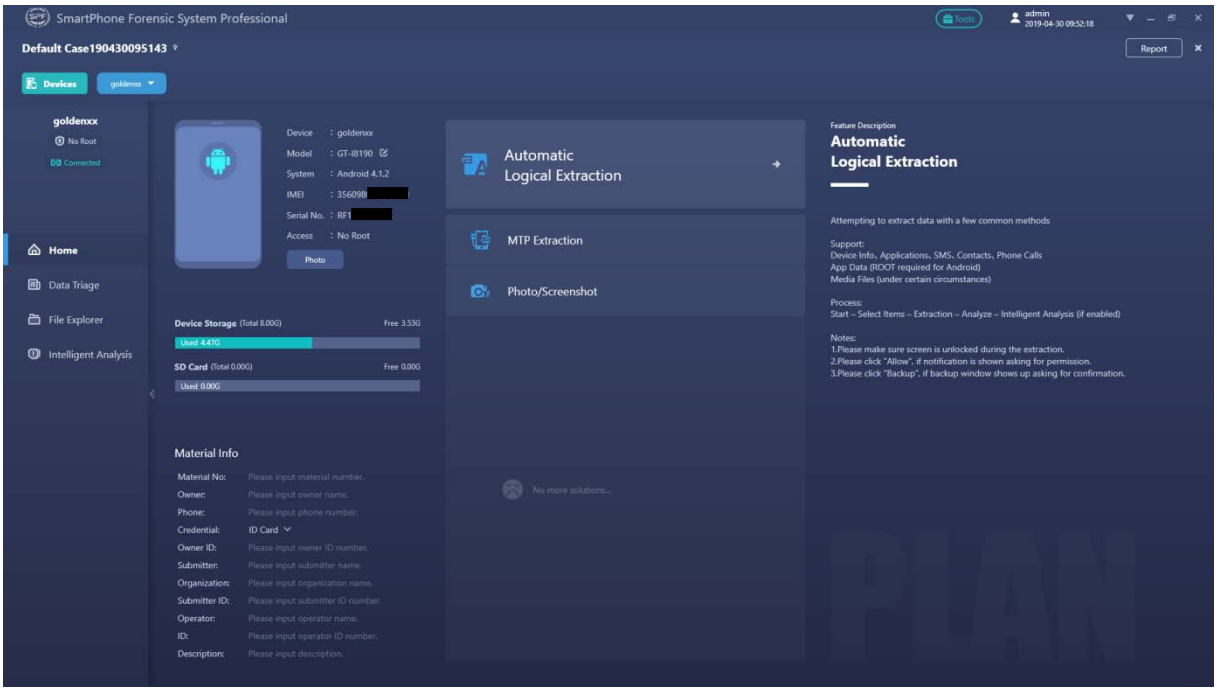
5.1. Forenzička analiza uređaja Samsung Galaxy S3 Mini

Samsung Galaxy S3 Mini još je poznat i kao Samsung I8190 Galaxy S3 mini. Razvijen je 2012. godine te predstavlja jeftinije i manje rješenje uređaja Samsung Galaxy S3. Karakteristike ovog uređaja su značajno slabije od novijih mobilnih uređaja. Radi na operativnom sustavu Android, a verzija Androida je 4.1. (Jelly Bean), što je jedna od starijih verzija, a *Chipset* na kojem radi je NovaThor U8420, [68]. Za potrebe diplomskog rada korištena su 2 uređaja Samsung Galaxy S3 Mini, od kojih je jedan *Root*-an, a drugi nije pa će se usporediti način ekstrakcije podataka i vidjeti utječe li *Root* pristup na mogućnosti ekstrakcije podataka.

Slika 11: Samsung Galaxy S3 Mini [69]

5.1.1. Samsung Galaxy S3 Mini bez ostvarenog Root pristupa

Kako bi se došlo do ekstrakcije podataka odnosno provedbe forenzičke analize, potrebno je zadovoljiti sve korake koji su objašnjeni u poglavlju 4. Sljedeća slika prikazuje informacije o mobilnom uređaju kao i mogućnosti ekstrakcije za uređaj Samsung Galaxy S3 Mini bez ostvarenog *Root* pristupa.



Slika 12: Informacije o mobilnom uređaju Samsung Galaxy S3 Mini bez ostvarenog Root pristupa te mogućnosti ekstrakcije podataka

Slika 12 gotovo je jednaka slici 8, no potrebno je za svaki mobilni uređaj prikazati mogućnosti ekstrakcije podataka. Na slici je vidljivo da se radi o mobilnom uređaju Samsung

Galaxy S3 Mini jer je model uređaja GT-I8190. Također vidljivo je da na uređaju nije ostvaren *Root* pristup te da je verzija Androida 4.1.2. (Jelly Bean).

Mogućnosti, tj. metode ekstrakcije podataka koje su dostupne za ovaj uređaj su jako male. Dostupne metode ekstrakcije za uređaj Samsung Galaxy S3 Mini bez ostvarenog *Root* pristupa su:

- Automatska logička ekstrakcija
- MTP (engl. *Media Transfer Protocol*) ekstrakcija
- Fotografija / Snimka zaslona

Automatska logička ekstrakcija prva je metoda koja je uglavnom dostupna na svim mobilnim uređajima. U poglavlju 3 detaljno je objašnjena logička ekstrakcija, a ova logička ekstrakcija zasniva se na komunikaciji s uređajem za preuzimanje odnosno ekstrakciju podataka s uređaja. Prilikom ovakve vrste ekstrakcije potrebno je da mobilni uređaj ima uključeno USB ispravljanje pogrešaka. Ovakva logička ekstrakcija spada u logičku ekstrakciju korištenjem ADB naredbi. Nakon što se na slici 12 odabrala automatska logička ekstrakcija odabiru se elementi koji će se ekstrahirati, a oni se odnose uglavnom na osnovne informacije o uređaju, SMS poruke, medijske zapise, i sl.

Ekstrakcija podataka sa svim svojim elementima, prikazana je na sljedećoj slici. Provođenje svih metoda koje su dostupne u alatu SPF Pro podrazumijeva ovaj korak i uključuje sve elemente kako je prikazano na slici.

Slika 13: Postupak ekstrakcije podataka

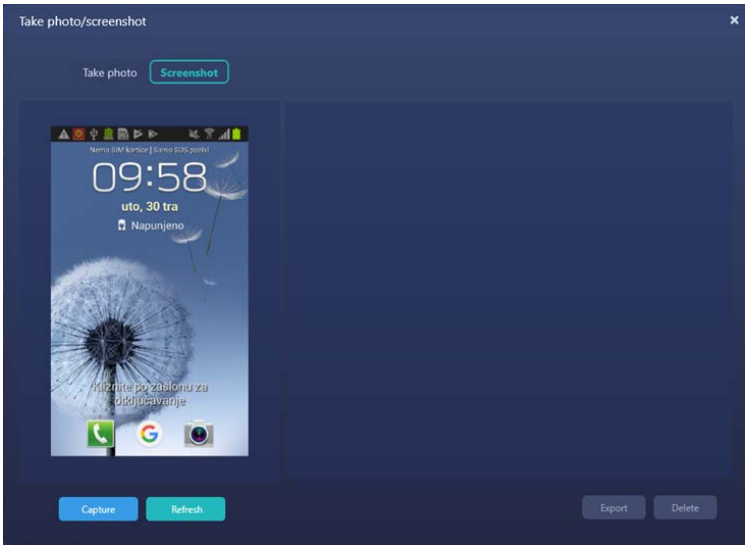
Slika 13 prikazuje zaslon ekrana u trenutku ekstrakcije podataka. Ekstrakcija nije zahtjevna za korisnika, odnosno on nema puno interakcije s računalom. Jedina interakcija

odnosi se na potvrdu za izradu sigurnosne kopije na mobilnom uređaju, a ta interakcija događa se na početku ekstrakcije podataka. Sam postupak ekstrakcije podataka sadrži sljedeće elemente:

1. Element naznačen kao 1 čine elementi koji se ekstrahiraju.
2. U djelu naznačenim kao 2 prikazuje se postotak svih podataka koji se trebaju ekstrahirati te ukupno vrijeme trajanja ekstrakcije.
3. Oznaka 3 sadrži broj podataka koji su se ekstrahirali, a u ovom slučaju je to 0 zato što je postupak ekstrakcije tek započeo.
4. Četvrti element prikazuje stanje u kojemu se nalaze elementi. Ono može biti čekanje (engl. *Waiting*) te završeno (engl. *Finished*).
5. Element naznačen kao 5 prikazuje vrijeme trajanja ekstrakcije za pojedini element.
6. Oznaka 6 prikazuje da je moguće prekinuti izvršavanje ekstrakcije klikom na tipku *Stop Acquisition*.

MTP (engl. *Media Transfer Protocol*) ekstrakcija isključivo se odnosi na medijske zapise pohranjene u mobilnom uređaju. Postupak ekstrakcije vrlo je sličan automatskoj logičkoj ekstrakciji i uključuje sve njene značajke, a to je vidljivo na slici 13. Ova metoda ekstrakcije neće pronalaziti niti ekstrahirati bilo kakve druge formate osim medijskih, stoga je ova metoda ekstrakcije dosta ograničena. Elementi koji se ekstrahiraju razlikuju se u odnosu na automatsku logičku ekstrakciju jer se odabiru samo medijski zapisi, a ne SMS-ovi, zapisi poziva, kalendari, i sl. Kao za automatsku logičku ekstrakciju, MTP te sve ostale ekstrakcije koje će se prikazati u ovome poglavlju, ekstrahirani podaci će se analizirati u poglavlju 6.

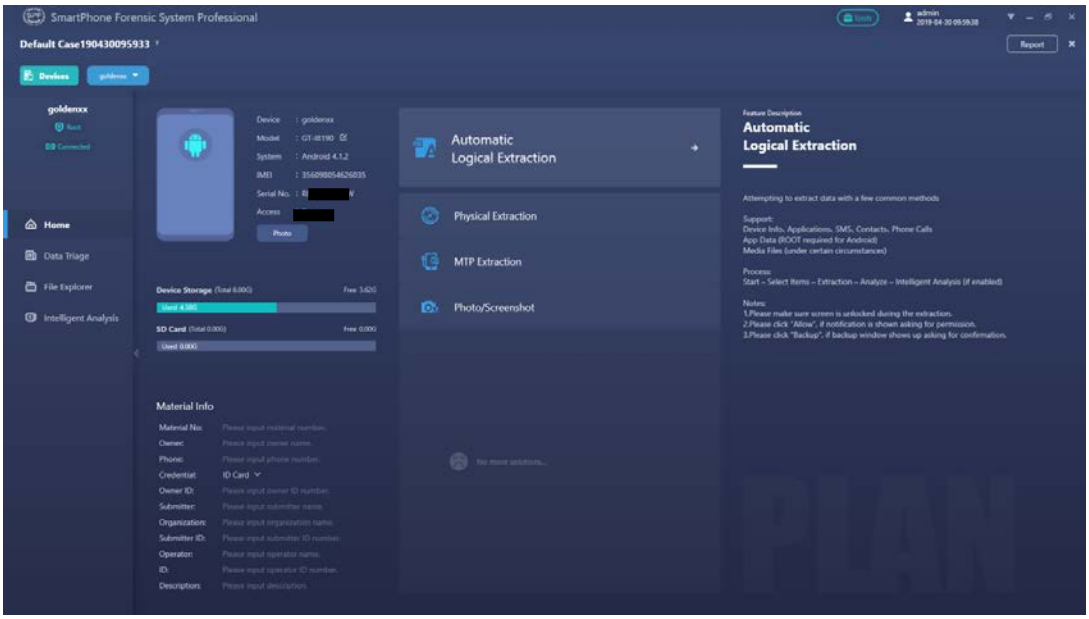
Fotografija / Snimka zaslona ne svrstava se u metode ekstrakcije podataka, no u nekim slučajevima ove mogućnosti mogu biti korisne. Prikazuje zaslon mobilnog uređaja u trenutku odabira tipke „*Capture*“ koja će biti vidljiva na sljedećoj slici. Snimka zaslona može biti korisna ako mobilni uređaj ima vanjsko oštećenje zaslona i nije moguće vidjeti što se događa na mobilnom uređaju. Ova mogućnost jednaka je na svim mobilnim uređajima.



Slika 14: Snimanje zaslona mobilnog uređaja Samsung Galaxy S3 Mini bez ostvarenog Root pristupa korištenjem alata SPF Pro

5.1.2. Samsung Galaxy S3 Mini s ostvarenim Root pristupom

Kao i za Samsung Galaxy S3 Mini koji nema ostvareni *Root* pristup i za ovaj uređaj s *Root* pristupom potrebno je zadovoljiti sve korake iz poglavlja 4. Ovaj uređaj *Root*-an je pomoću alata KingoRoot koji se nalazi u sklopu alata SPF Pro. Sljedeća slika prikazat će razliku između uređaja koji ima ostvaren *Root* pristup i uređaja koji nema.



Slika 15: Informacije o mobilnom uređaju Samsung Galaxy S3 Mini s ostvarenim *Root* pristupom te mogućnosti ekstrakcije podataka

Slika 15 prikazuje osnovne informacije o mobilnom uređaju. Sve informacije su jednake kao na slici 12 osim dijela gdje se prikazuje je li uređaj *Root*-an ili nije. SPF Pro se može koristiti kao alat za provjeru *Root* statusa na mobilnom uređaju. Metode ekstrakcije podataka su znatno različite u odnosu na uređaj bez *Root* pristupa. Ovaj uređaj ima jednu metodu ekstrakcije više, a to je fizička ekstrakcija. Fizička ekstrakcija metoda je koja može ekstrahirati najveću količinu podataka iz mobilnih uređaja pa se može zaključiti da na mogućnosti alata SPF Pro utječe *Root* status mobilnog uređaja.

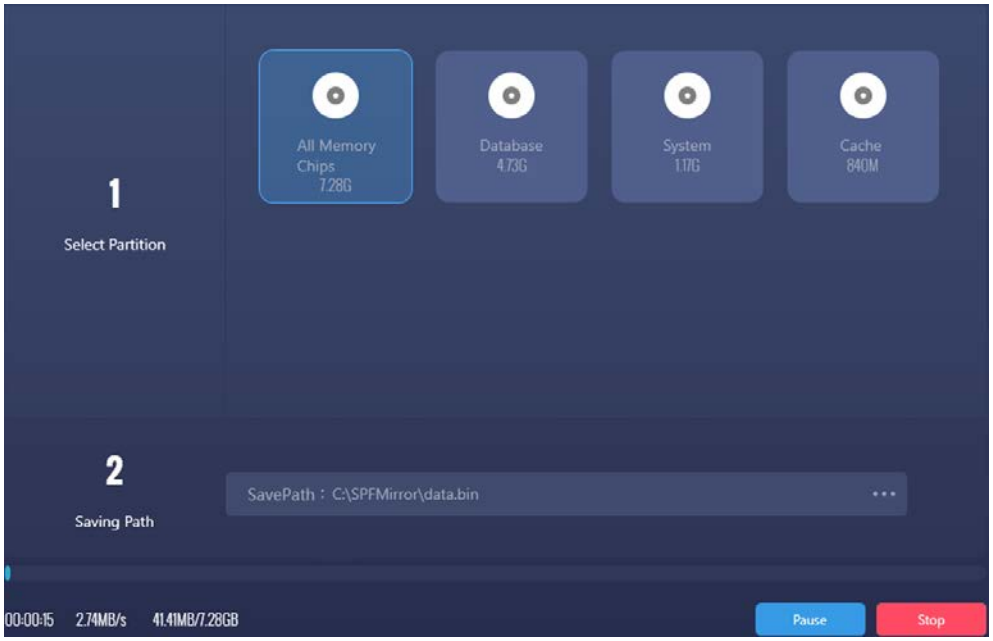
Moguće metode ekstrakcije koje se mogu primijeniti na mobilni uređaj Samsung Galaxy S3 Mini s ostvarenim *Root* statusom su:

- Automatska logička ekstrakcija
- **Fizička ekstrakcija**
- MTP (engl. *Media Transfer Protocol*) ekstrakcija
- Fotografija / Snimka zaslona

Automatska logička ekstrakcija za *Root*-ani Samsung Galaxy S3 Mini provodi se na identičan način kao i za uređaj koji nema ostvaren *Root* pristup. Postupak ekstrakcije nalazi se

na slici 13. Ekstrahirani podaci te količina ekstrahiranih podataka bit će uspoređena u poglavlju 6.

Fizička ekstrakcija je metoda koja nije bila prisutna u uređaju bez *Root* pristupa. Kao što je navedeno u poglavlju 3, fizička ekstrakcija najzahtjevnija je i najdugotrajnija metoda ekstrakcije podataka. Sam postupak ekstrakcije znatno se razlikuje od automatske logičke ekstrakcije i MTP ekstrakcije, no postupak fizičke ekstrakcije ih uključuje, a on je prikazan na u nastavku. Također kod fizičke ekstrakcije potrebno je zadovoljiti sve prethodne korake kao što su otvaranje novog slučaja, povezivanje uređaja, i sl.



Slika 16: Mogućnosti provođenja fizičke ekstrakcije

Na slici 16 moguće je vidjeti mogućnosti ekstrahiranja pojedinih izvora digitalnih dokaza mobilnih uređaja. Prvi korak predstavlja odabir particije koja će se ekstrahirati. Vidljivo je da svi memorijski čipovi (engl. *All Memory Chips*) imaju najveću mogućnost pohrane, odnosno sadrže najveću količinu podataka, a ona iznosi 7,28 GB. Uz to, moguće je izvršiti ekstrakciju baza podataka, sistemskih podataka te *Cache* memorije. Nakon što se odabere particija koja se želi ekstrahirati, potrebno je odrediti putanju pohrane. Važno je naglasiti da se tu pohranjuje preslika memorije, a ne sami podaci. Alat SPF Pro kod fizičke ekstrakcije ne ekstrahira podatke direktno iz navedenih particija, već prvo radi presliku svake od njih. Nakon što je preslika ili drugim nazivom forenzička slika određene particije uspješno izvršena potrebno je napraviti ekstrakciju te preslike. Na taj način se primjenjuje fizička ekstrakcija u alatu SPF Pro. Ekstrakcija preslike provodi se jednako kao i bilo koja metoda ekstrakcije podataka mobilnih uređaja, isključujući fizičku ekstrakciju. Nakon što je preslika određenog dijela memorije otvorena, potrebno je odabrati metodu ekstrakcije podataka. Moguće je izvršiti automatsku logičku ekstrakciju, MTP ekstrakciju (koja se u ovom slučaju naziva *Media File Extraction*) te snimiti zaslon mobilnog uređaja. Provođenje ovih dostupnih metoda ekstrakcije uvijek se izvodi istim postupkom, a taj postupak vidljiv je na slici 13.

Nakon što je ekstrakcija preslike određenog dijela memorije uspješno izvršena, slijedi analiza ekstrahiranih podataka. U poglavlju 6 bit će prikazani ekstrahirani podaci, a njihova količina nakon provedbe fizičke ekstrakcije znatno se razlikuje u odnosu na druge metode ekstrakcije, što je i očekivano.

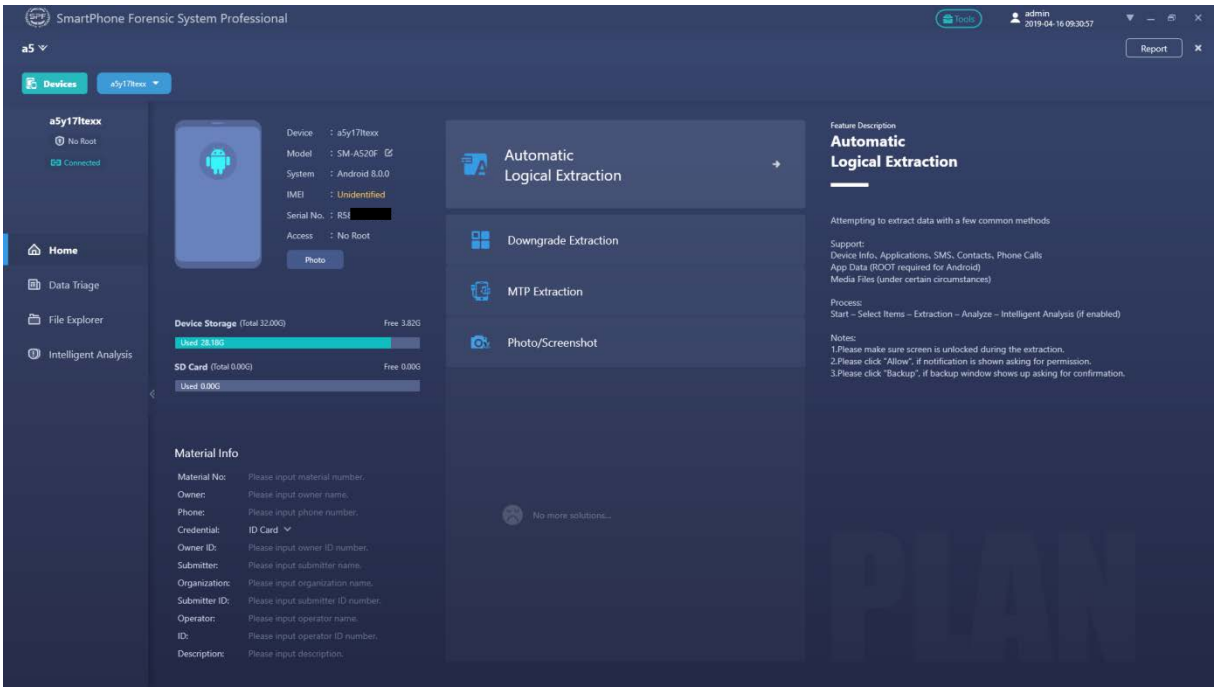
MTP ekstrakcija te **Fotografija / Snimka zaslona** za *Root*-ani uređaj Samsung Galaxy S3 mini provode se na identičan način kao i za uređaj koji nije *Root*-an. Količina ekstrahiranih podataka za MTP ekstrakciju bit će prikazana u idućem poglavlju. MTP ekstrakcija te snimke zaslona uređaja provode se jednako za sve uređaje, a njihov način je prethodno opisan.

5.2. Forenzička analiza uređaja Samsung Galaxy A5

Samsung Galaxy A5 moguće je pronaći u sljedećim verzijama: A520F (Europsko tržište, *Single* - SIM), a to je verzija koja se koristi u ovom diplomskom radu, A520F/DS (Globalno tržište, *Dual* – SIM), A520K/L/S (Južna Korea). Razvijen je 2017. godine i po karakteristikama je te godine mogao parirati drugim uređajima. Često mu se uz naziv piše i godina proizvodnje (Samsung Galaxy A5 2017) jer postoji isti uređaj godinu stariji. U današnje vrijeme, Samsung Galaxy A5 je financijski prihvatljiv i karakteristikama zadovoljavajuć za izvršavanje svakodnevnih radnji. Operativni sustav na kojem radi je Android, a podržava verzije od 6.0.1. (Marshmallow) do 8.0.0. (Oreo). Uređaj koji se koristi za potrebe diplomskog rada radi na verziji 8.0.0. (Oreo), [70].

Slika 17: Samsung Galaxy A5 [71]

Ovaj mobilni uređaj znatno je noviji od Samsung Galaxy S3 Mini uređaja te radi na novijem operativnom sustavu. Iz tog razloga postoje neke razlike u informacijama o uređaju te metodama ekstrakcije unutar alata SPF Pro. Kao i na prošlim uređajima, potrebno je kreirati slučaj kako bi se ekstrakcija podataka mogla izvesti. Ovaj uređaj nema ostvareni *Root* pristup što će biti vidljivo na sljedećoj slici.



Slika 18: Informacije o mobilnom uređaju Samsung Galaxy A5 te mogućnosti ekstrakcije podataka

Slika 18 prikazuje osnovne informacije te metode ekstrakcije te predstavlja sučelje koje je jednako za svaki mobilni uređaj. Informacije i dostupne metode ekstrakcije se razlikuju, što je i očekivano, jer se mobilni uređaji razlikuju prema mnoštvu elemenata, kao što je to *Root* status, verzija operativnog sustava, proizvođač, i sl. Na slici je vidljivo da se radi o modelu uređaja SM-A520F, a to je upravo Samsung Galaxy A5. Također je vidljivo da uređaj nema ostvaren *Root* pristup te da IMEI nije moguće prikazati. Razlog tomu je što SPF Pro različito radi s novijim operativnim sustavima, a i noviji operativni sustavi imaju veću zaštitu samog uređaja pa je prepoznavanje IMEI-a u ovom slučaju neuspješno odrađeno.

Mogućnosti ekstrakcije podataka koje su dostupne za uređaj Samsung Galaxy A5 vidljive su na slici 18. Jedina ekstrakcija koja se nije pojavila kod uređaja Samsung Galaxy S3 Mini je Downgrade Ekstrakcija. Načini na koje se podaci mobilnih uređaja mogu ekstrahirati su:

- Automatska logička ekstrakcija
- **Downgrade ekstrakcija**
- MTP Ekstrakcija
- Fotografija / Snimka zaslona

Postupak provođenja **Automatske logičke ekstrakcije** jednak je za sve uređaje kao što je navedeno, no količina ekstrahiranih podataka znatno se razlikuje. O toj temi bit će govora u poglavlju 6. Postupak automatske logičke ekstrakcije nalazi se na slici 13.

Downgrade ekstrakcija se odnosi na spuštanje odnosno nadogradnju aplikacija na nižu verziju s ciljem zaobilaženja određenih zaštita, a u svrhu lakše ekstrakcije određenih

podataka. Ona se može primijeniti na Android uređajima koji rade na operativnom sustavu verzije 7 ili više. Ova metoda ekstrakcije vrlo je rizična jer se njome mogu trajno izgubiti vrijedni podaci pohranjeni na mobilnom uređaju. Jedan od ključnih koraka ove metode ekstrakcije podataka je deinstaliranje izvorne aplikacije bez dodirivanja korisničkih podataka. Nakon što se na slici 18 odabere Downgrade ekstrakcija, odabiru se elementi koji će se ekstrahirati. Odabir elemenata izvodi se na isti način kao i u automatskoj logičkoj ekstrakciji, samo se u ovom slučaju odabiru elementi koji su usmjereni društvenim mrežama te platformama za komunikaciju.

Sam postupak ekstrakcije vrlo je sličan onome u automatskoj logičkoj ekstrakciji, vidljivoj na slici 13. Razlika je u elementima koji se ekstrahiraju jer se ovdje uglavnom pokušavaju dobaviti podaci društvenih mreža i komunikacije iz raznih platformi. Također, ova metoda ekstrakcije uključuje interakciju s mobilnim uređajem. Na završetku ekstrakcije prikazuje se prozor „Info“ koji govori da je uređaj ponovno pokrenut te da je potrebno otključati zaslon, pratiti obavijesti i dopustiti pristup za početak Downgrade ekstrakcije. Ova metoda ekstrakcije ponovljena je nekoliko puta na mobilnom uređaju Samsung Galaxy A5. Gotovo svaka ekstrakcija je imala drugačiji ishod, odnosno u nekima od njih se ekstrakcija prekinula jer se nisu mogli pronaći podaci unutar određenih aplikacija kao što je to bio slučaj za „Google Maps“. Također, ako se odaberu elementi koje mobilni uređaj ne sadrži, odnosno da te aplikacije ne postoje u mobilnom uređaju, ekstrakcija će se prekinuti. Pozitivna strana je što će se moći analizirati podaci koji su do trenutka prekida bili ekstrahirani. Količina i vrsta ekstrahiranih podataka bit će prikazana u poglavlju 6.

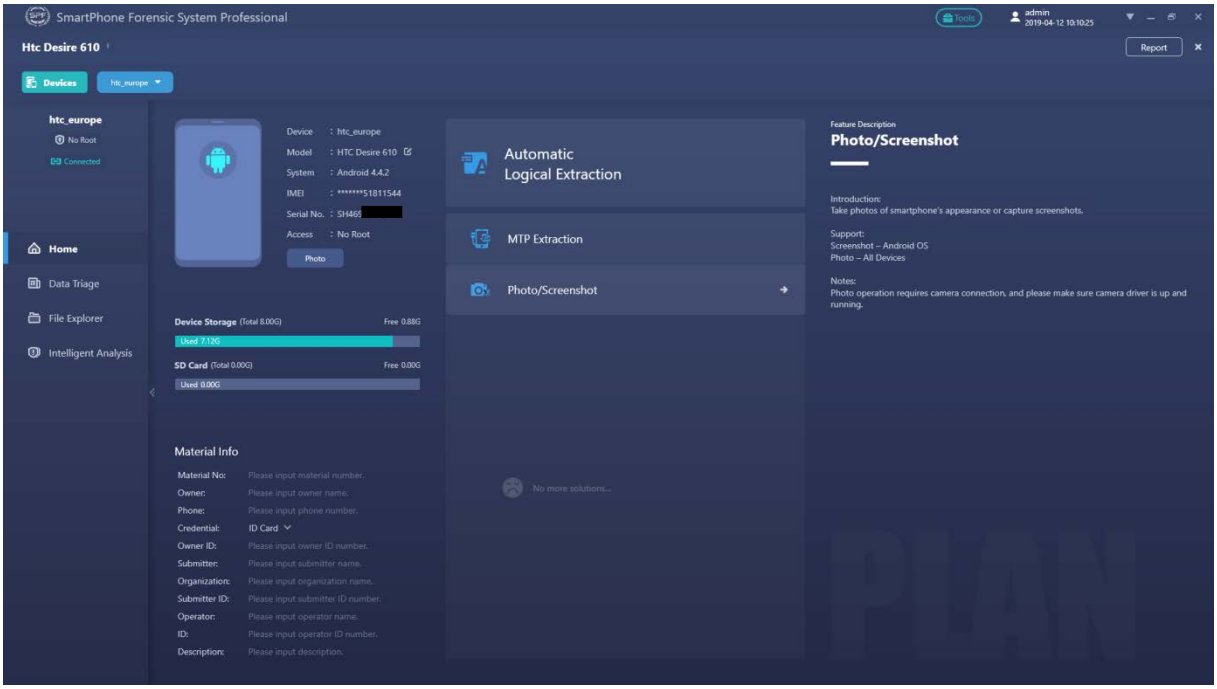
MTP ekstrakcija te **Fotografija / Snimka zaslona** za uređaj Samsung Galaxy A5 provodi se na identičan način kao i za sve ostale uređaje. Količina ekstrahiranih podataka za MTP ekstrakciju bit će prikazana u idućem poglavlju. MTP ekstrakcija te snimke zaslona uređaja jednake su za sve mobilne uređaje, ali treba uzeti u obzir da snimka zaslona na slici 14 nije jednaka snimci zaslona uređaja Samsung Galaxy A5, što je i logično jer su različiti uređaji, no postupak je potpuno jednak.

5.3. Forenzička analiza uređaja HTC Desire 610

HTC Desire 610 mobilni je uređaj koji je razvijen 2014. godine. U usporedbi s današnjim mobilnim uređajima može se reći da je ovaj uređaj zastario, odnosno ima nešto slabije performanse. Ovaj uređaj koji se koristi za potrebe diplomskog rada radi na operativnom sustavu Android, verzije 4.4.2 (KitKat), [72].

Slika 19: HTC Desire 610 [73]

Ovaj uređaj nema omogućen *Root* pristup, stoga se ne mogu očekivati brojne mogućnosti za ekstrakciju podataka. Verzija operativnog sustava Android ovog uređaja nešto je novijeg datuma od verzije uređaja Samsung Galaxy S3 Mini, pa se mogu očekivati približno jednake mogućnosti za ekstrakciju podataka te prikaz informacija o uređaju.



Slika 20: Informacije o mobilnom uređaju HTC Desire 610 te mogućnosti ekstrakcije podataka

Na slici 20 prikazane su osnovne informacije i mogućnosti ekstrakcije podataka za uređaj HTC Desire 610, a kao što je i navedeno, vrlo je slična slici 12 koja se odnosi na Samsung Galaxy S3 Mini bez ostvarenog *Root* pristupa. Sve informacije o mobilnom uređaju jednake su kao i kod Samsung Galaxy S3 Mini-a osim podatka o IMEI-u, koji ima prikrivenih nekoliko znamenki, što predstavlja dobru zaštitu samog uređaja.

Metode ekstrakcije koje su dostupne za uređaj HTC Desire 610 su:

- Automatska logička ekstrakcija
- MTP (engl. *Media Transfer Protocol*) ekstrakcija
- Fotografija / Snimka zaslona

Metode ekstrakcije jednake su kao i za uređaj Samsung Galaxy S3 Mini bez ostvarenog *Root* pristupa, a jednak je i postupak svake metode za ekstrakciju podataka. Za **automatsku logičku ekstrakciju** postupak provedbe ekstrakcije nalazi se na slici 13. **MTP ekstrakcija** te njen postupak provedbe uvijek je jednak postupku automatske logičke ekstrakcije pa i za ovu metodu ekstrakciju vrijedi postupak na slici 13., a **Snimku Zaslona**, odnosno postupak snimke zaslona moguće je vidjeti na slici 14, no kao i kod uređaja Samsung Galaxy A5 ona nije jednaka. U poglavlju 6 prikazat će se količina ekstrahiranih podataka za svaku pojedinu metodu.

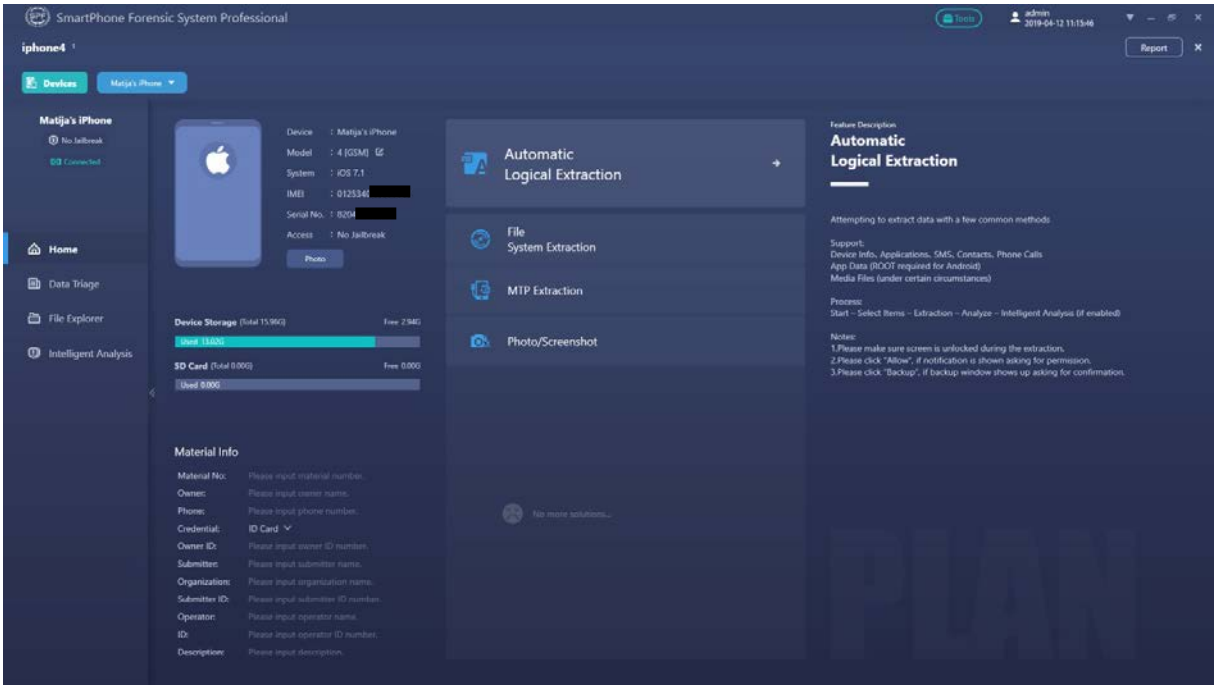
5.4. Forenzička analiza uređaja iPhone 4

iPhone 4 predstavlja četvrtu generaciju Apple-ovog mobilnog uređaja iPhone koji je razvijen 2010. godine. U svoje vrijeme bio je jedan od najboljih mobilnih uređaja na tržištu po karakteristikama te dizajnu. U četvrtu generaciju svrstava se i poboljšana verzija iPhon-a 4, a to je iPhone 4s koji ima značajne prednosti u odnosu na iPhone 4, a najveća je prednost nadogradnja operativnog sustava do verzije iOS 9.3.5. Verzija iOS operativnog sustava na kojem iPhone 4 može raditi varira od iOS 4.0 do iOS 7.1.2. Mobilni uređaj koji se koristi za potrebe ovog diplomskog rada, radi na verziji 7.1, [74].

Slika 21: iPhone 4, [75]

Ovaj mobilni uređaj nema omogućen potpuni pristup operativnom sustavu iOS (tzv, *Jailbreak*). *Jailbreak* se može poistovjetiti s *Root*-om koji se koristi za potpuni pristup operativnom sustavu Android. iPhone 4 prvi je uređaj u ovom radu koji ne radi na

operativnom sustavu Android pa će se iz tog razloga metode i mogućnosti ekstrakcije u nekim dijelovima razlikovati. Kao i kod Android uređaja, potrebno je zadovoljiti sve prethodne korake kao što su prepoznavanje uređaja i kreiranje slučaja, a koji su uvijek jednaki.



Slika 22: Informacije o mobilnom uređaju iPhone 4 te mogućnosti ekstrakcije podataka

Slika 22 prikazuje osnovne informacije te mogućnosti ekstrakcije podataka uređaja iPhone 4. Za razliku od Android uređaja, moguće je primijetiti neke razlike, a najuočljivija je logo samog uređaja. Ostale informacije su vrlo slične kao i za prethodne uređaje te je vidljivo da uređaj nema ostvaren potpuni pristup operativnom sustavu, odnosno *jailbreak.* U potpunosti su vidljivi IMEI te serijski broj uređaja, a što može naslutiti da će se ekstrahirati veća količina značajnih podataka.

Određene metode ekstrakcije podataka slične su kao i za Android uređaje, no ipak postoje određene razlike koje će biti prikazane u nastavku. Omogućena je jedna nova metoda ekstrakcije a to je *File System Extraction* odnosno datotečna ekstrakcija. Metode ekstrakcije podataka koje su dostupne za mobilni uređaj iPhone 4 su:

- Automatska logička ekstrakcija
- **Ekstrakcija datotečnog sustava / Datotečna ekstrakcija**
- MTP (engl. *Media Transfer Protocol*) ekstrakcija
- Fotografija / Snimka zaslona

Automatska logička ekstrakcija jednostavna je metoda koja je dostupna za sve mobilne uređaje pa tako i za iOS uređaje. Kao i kod Android uređaja, potrebno je da je USB ispravljanje pogrešaka uključeno jer u protivnom ekstrakcija podataka neće biti moguća. Postupak kojim se dolazi do ekstrakcije podataka vrlo je sličan onome za Android uređaje, no ipak postoji mala razlika. Ta razlika očituje se u izboru elemenata koji će se ekstrahirati jer

određeni elementi neće biti ponuđeni na odabir zato što mogu biti instalirani samo na Android uređajima. Određeni elementi mogu se odabrati samo za iOS uređaje, a iz istog razloga kao što je to za elemente Android uređaja. Nakon što su elementi odabrani, slijedi ekstrakcija tih podataka. Postupak ekstrakcije podataka jednak je za sve uređaje pa tako i za iPhone 4, a postupak je vidljiv na slici 13. Za sve uređaje postupak uključuje interakciju korisnika, odnosno potvrdu za izradu sigurnosne kopije. Podaci koji su ekstrahirani bit će analizirani i prikazani u poglavlju 6.

Ekstrakcija datotečnog sustava / Datotečna ekstrakcija obuhvaća sve datoteke koje su pohranjene u memoriji mobilnog uređaja. Provođenje ove metode ekstrakcije vremenski traje duže u odnosu na logičku ekstrakciju jer se pronalaze i ekstrahiraju sve datoteke u mobilnom uređaju, a njihov broj je velik. Moguće je odabrati jedan element za ekstrakciju, a to je *Database,* odnosno baze podataka što je sasvim logično jer datotečna ekstrakcija pretražuje datoteke. Odabir tog elementa i početak ekstrakcije izvode se na isti način kao i kod fizičke ekstrakcije, što je vidljivo na slici 16. Važno je naglasiti da se podaci ne ekstrahiraju odmah nego se prvo radi forenzička slika određenog dijela memorije, što u ovom slučaju predstavljaju baze podataka. Nakon što je forenzička slika kreirana potrebno ju je otvoriti, a zatim se odabire metoda kojom će se ona ekstrahirati. Na isti način provodi se i ekstrakcija forenzičke slike koja je nastala u sklopu fizičke ekstrakcije. Ekstrakcija preslike odnosno forenzičke slike provodi se na isti način kao i provođenje bilo koje metode ekstrakcije nad određenim mobilnim uređajem. Metode koje su dostupne za ekstrakciju forenzičke slike baze podataka jednake su kao i u fizičkoj ekstrakciji, a to su automatska logička ekstrakcija, *Media File Extraction* odnosno MTP ekstrakcija te snimka zaslona mobilnog uređaja. Te metode uvijek se izvode na isti način za sve mobilne uređaje i forenzičke slike određenog dijela memorije. Ekstrahirani podaci svake metode bit će prikazani i uspoređeni u sljedećem poglavlju.

MTP ekstrakcija te **Snimka zaslona** jednake su za sve mobilne uređaje. Iako se u ovom slučaju radi o mobilnom uređaju s drugačijim operativnim sustavom, nego je to bilo slučaj kod prethodna tri uređaja, ekstrahiranje te snimanje zaslona potpuno su jednaki.

6. Validacija i analiza ekstrahiranih podataka

Ovo poglavlje usmjereno je analizi ekstrahiranih podataka do kojih se došlo provođenjem različitih metoda ekstrakcije za pojedine mobilne uređaje, što je prikazano u poglavlju 5. Ovaj korak u forenzičkoj analizi je najbitniji jer svi postupci koji su se morali odraditi u poglavlju 4 i poglavlju 5 imali su samo jedan cilj, a to je ekstrahirati podatke iz mobilnih uređaja te potencijalno pronaći vrijedne digitalne dokaze. Analiza podataka u alatu SPF Pro vrlo je jednostavna, no neke mogućnosti analize za obrađene mobilne uređaje uopće ne rade ili ne rade na način na koji bi trebale, a što će biti vidljivo u narednim poglavljima i slikama.

6.1. Mogućnosti analize ekstrahiranih podataka

Softverski alat SPF Pro nudi tri mogućnosti analize i pregledavanja ekstrahiranih podataka. Kao što je navedeno, za pojedine mobilne uređaje ne rade ispravno. Uz dostupne analize moguće je kreirati izvještaj u kojemu se nalaze ekstrahirani podaci. Mogućnosti analize ekstrahiranih podataka koje će biti spomenute u nastavku rada su:

- Obrada podataka (engl. *Data Triage*)
- Preglednik datoteka (engl. *File Explorer*)
- Pametno pretraživanje (engl. *Intelligent Analysis*)

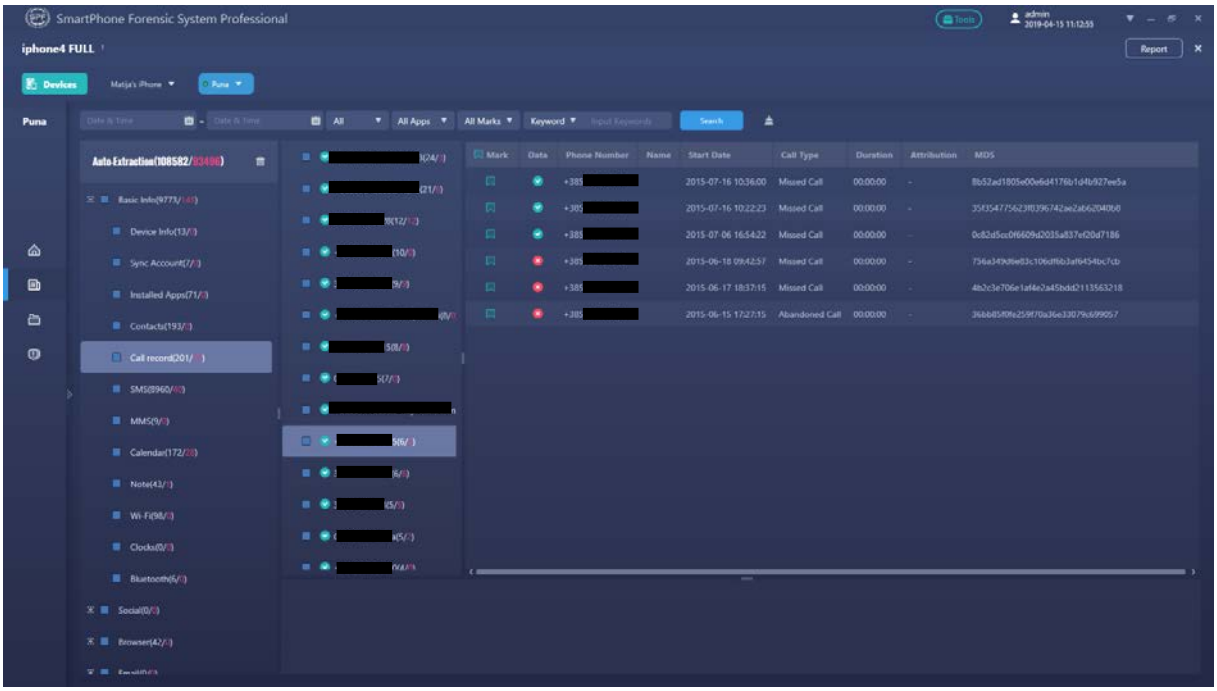
6.1.1. Obrada podataka

Obrada podataka odnosno trijažni postupci osnovni je način analize podataka unutar alata SPF Pro. Ovaj način obrade podataka pokreće se automatski, odmah nakon što je ekstrakcija provedena. Radi na lako razumljiv način te uz jednostavno sučelje omogućava jednostavan pregled ekstrahiranih podataka. Prikazuje izbrisane podatke za pojedini izvor podataka, no količina izbrisanih podataka koji su ekstrahirani ovisi o modelu uređaja, verziji operativnog sustava te metodi ekstrakcije. Ovaj način analize podataka dostupan je za svaki obrađeni mobilni uređaj, a način na koji se analiza vrši prikazan je na sljedećoj slici.

6.1.1.1. Obrada podataka ekstrahiranih automatskom logičkom ekstrakcijom

Obrada podataka ekstrahiranih automatskom logičkom ekstrakcijom prikazana je na slikama 23 i 24, a analiza tih podataka je najdugotrajnija jer sadrži najviše izvora podataka koji su se ekstrahirali. U prethodnom poglavlju objašnjen je način provedbe ove ekstrakcije,

ali i fizičke i datotečne ekstrakcije koje kreiraju forenzičku sliku, a koja se zatim ekstrahira automatskom logičkom ili MTP ekstrakcijom. Iz tog razloga fizičku i datotečnu ekstrakciju nema potrebe potkrepljivati slikama jer njihov postupak analize uključuje automatsku logičku i MTP ekstrakciju. Sljedeća slika prikazuje sučelje alata SPF Pro tijekom analize podataka ekstrahiranih logičkom ekstrakcijom.



Slika 23: Obrada podataka ekstrahiranih logičkom ekstrakcijom

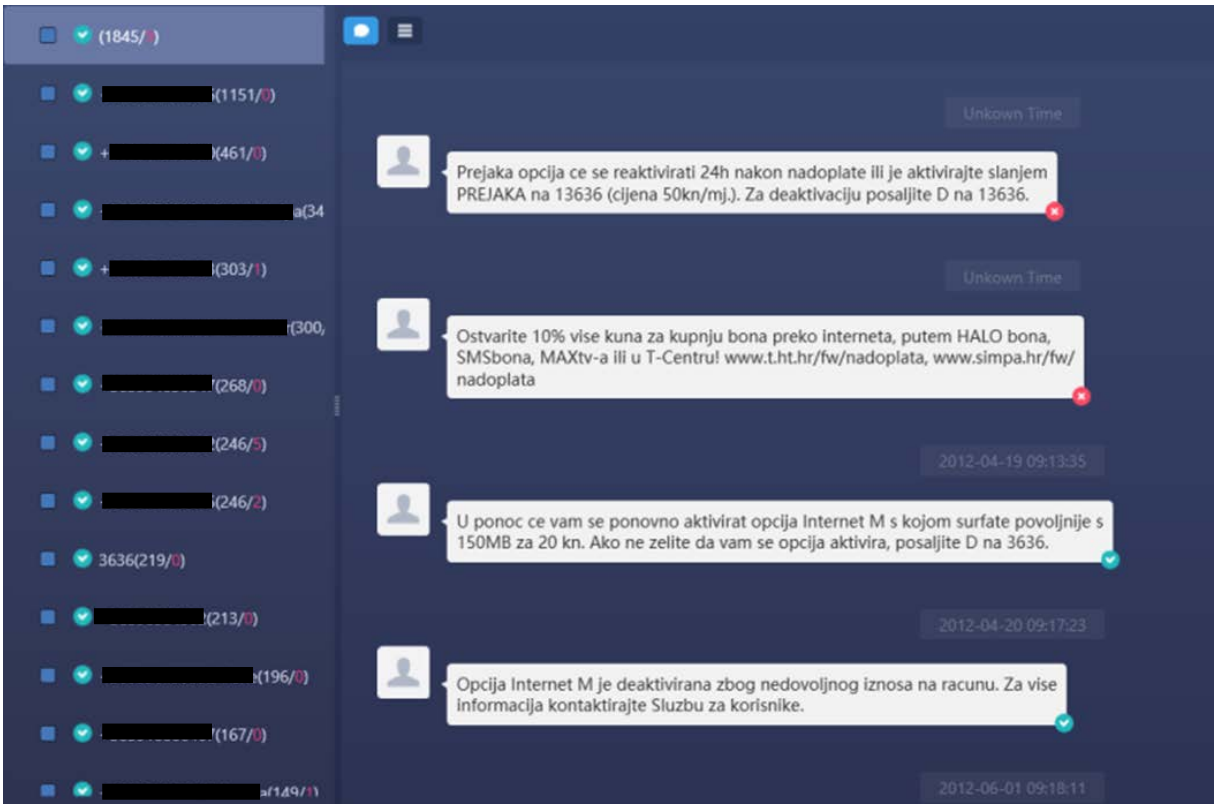
Slika 23 prikazuje sučelje kojim se izvodi obrada podataka (engl. *Data Triage*) automatske logičke ekstrakcije, a vidljivo je da se to izvršava na jednostavan i lako razumljiv način. Na slici je vidljivo da se s lijeve strane prikazuju ekstrahirani podaci za pojedine izvore podataka gdje prvi broj u zagradi označava ukupnu količinu podataka, a drugi koji je naznačen crvenom bojom označava broj izbrisanih podataka. Elementi koji su prikriveni odnose se na kontakte i njihove telefonske brojeve, a prikrivaju se radi očuvanja privatnosti. Svi izvori podataka su u takvom formatu, a takav prikaz ekstrahiranih podataka vrlo je sličan u ostalim forenzičkim alatima iste namjene. S desne strane sučelja uvijek se prikazuju pojedinosti o pojedinim ekstrahiranim podacima. Nad svim ekstrahiranim podacima moguće je izvršiti pretragu prema ključnim riječima, datumu, prema određenoj aplikaciji ili oznaci.

Forenzički alat SPF Pro podijelio je izvore podataka automatske logičke ekstrakcije po kategorijama, a prva od njih su osnovne informacije (engl. *Basic Info*). Tih elemenata, odnosno izvora podataka ima najviše, a to su:

- **Informacije o uređaju** (engl. *Device Information*) – Sadrži informacije o serijskom broju mobilnog uređaja, broju SIM kartice, nazivu uređaja, proizvođaču, modelu

uređaja, operativnom sustavu te njegovoj verziji, *Root-u* odnosno *Jailbreak* statusu, IMEI-u i sl. Te informacije nije moguće izbrisati pa ih tako i forenzički alat SPF Pro ne može prikazati kao izbrisane.

- **Sinkroniziranje računa** (engl. *Sync Account*) – Podaci o sinkroniziranju računa dostupni su samo za iOS uređaje, a SPF Pro prikazuje osnovne informacije o računu koji se odnosi na *iTunes*, a koristi se i za *Apple Store*.
- **Instalirane aplikacije** (engl. *Installed Apps*) – Sadrži sve aplikacije instalirane na mobilnom uređaju gdje je prikazan njihov naziv, instalirana verzija te putanja pohrane. One mogu biti izbrisane, a SPF Pro ih označava kao izbrisane na isti način kako je vidljivo na slici 23 gdje su prikazani izbrisani zapisi poziva. SPF Pro nije ekstrahirao izbrisane aplikacije ni za jedan uređaj koji se koristio za potrebe izrade ovog diplomskog rada.
- **Kontakti** (engl. *Contacts*) – Kontakti mogu biti izbrisani, a SPF Pro ih prikazuje jednako kao i za bilo koji drugi izvor podataka. SPF Pro automatskom logičkom ekstrakcijom nije ekstrahirao niti jedan izbrisani kontakt za sve mobilne uređaje koji su korišteni, što mu je još jedan veliki nedostatak. Informacije koje su ekstrahirane o kontaktima sadrže telefonski broj određenog kontakta, njegov naziv u mobilnom uređaju, grupu (ako je svrstan u nju), zadnji kontakt s tim kontaktom, te MD5 *Hash* vrijednost pojedinog kontakta.
- **Zapisi poziva** (engl. *Call Record*) – Slika 23 prikazuje ekstrahirane podatke o zapisima poziva te njihove pojedinosti. Tako forenzički alat SPF Pro ekstrahira pozive za pojedinog kontakta ili pojedini broj kontakta. Za njih se prikazuju broj mobilnog uređaja, naziv kontakta, datum poziva, vrsta poziva (odlazni, dolazni, odbijeni ili propušteni), trajanje poziva te MD5 *Hash* vrijednost. Podaci o zapisima poziva mogu biti izbrisani što je također vidljivo na slici 23.
- **SMS** (engl. *Short Message Service*) / **MMS** (engl. *Multimedia Message Service*) – Forenzički alat SPF Pro automatskom logičkom ekstrakcijom ekstrahira primljene ili poslane SMS i MMS poruke. SPF Pro također sadrži grafičko sučelje na kojem je vidljiv tekst poruke za pojedinog kontakta, a on je prikazan na slici 24. Za izradu diplomskog rada kontakti su prikriveni radi očuvanja privatnosti. Alat ekstrahira i izbrisane poruke, a one su naznačene crvenim znakom x, što je također vidljivo na sljedećoj slici.



Slika 24: Obrada podataka SMS i MMS poruka grafičkim sučeljem

- **Kalendar** (engl. *Calendar*) – Informacije o kalendaru koje SPF Pro forenzički alat ekstrahira automatskom logičkom ekstrakcijom mogu biti vrlo značajne jer osumnjičena osoba može u kalendaru naznačiti datum u kojem se izvršila ili će se izvršiti određena zlonamjerna aktivnost. Analizom kalendara mogu se utvrditi naziv određene aktivnosti za taj datum, postavljena lokacija, opis, datum i MD5 *Hash* vrijednost. Zapisi u kalendaru mogu biti izbrisani, a SPF Pro ih može ekstrahirati.
- **Bilješke** (engl. *Notes*) – Podaci o bilješkama ekstrahiraju se samo za iOS uređaje, a analizom se mogu utvrditi osnovne informacije o njima. Za pojedinu bilješku prikazuje se naziv bilješke, tekst bilješke, datum izrade te MD5 *Hash* vrijednost. Bilješke mogu biti izbrisane, a SPF Pro ih je uspio ekstrahirati za uređaj iPhone 4.
- **Wi-Fi** – Podaci ekstrahirani o Wi-Fi konekcijama prikazuju naziv mreže na koju je uređaj bio povezan, lozinku s kojom je pristupio toj mreži, vrstu konekcije te MD5 *Hash* vrijednost, a ti podaci mogu biti vrlo korisni za pronalaženje određene osumnjičene osobe. Te konekcije su na određenim mobilnim uređajima koji se koriste za potrebe diplomskog rada izbrisane, no SPF Pro ih nije ekstrahirao što predstavlja također još jedan nedostatak.
- **Satovi** (engl. *Clocks*) – Ovi podaci odnose se na alarme koji se postavljaju u pojedinom mobilnom uređaju. Niti jedna ekstrakcija koja je provedena na mobilnim uređajima nije ekstrahirala podatke o njima, što također dodaje alatu SPF Pro još jedan nedostatak.

- ***Bluetooth*** – SPF Pro ekstrahira podatke o *Bluetooth* konekcijama, a analizom se mogu utvrditi informacije o MAC adresi uređaja s kojim je ostvarena konekcija, vrsti uređaja o kojem se radi (mobilni uređaj, *Bluetooth* slušalice ili *Bluetooth* zvučnik, itd.), datumu zadnje konekcije te MD5 *Hash* vrijednost. *Bluetooth* konekcije nije jednostavno izbrisati pa tako na uređajima koji su obrađeni za potrebe ovog diplomskog rada ti podaci nisu izbrisani, a ih iz tog razloga forenzički alat SPF Pro nije ekstrahirao.

Sljedeća kategorija nije ekstrahirana automatskom logičkom ekstrakcijom ni za jedan mobilni uređaj što je također nedostatak alata SPF Pro. To je kategorija Društveni sadržaji (engl. *Social*), a taj izvor podataka trebao bi prikazati pojedinosti o društvenim mrežama i komunikacijama koje se njima odvijaju. SPF Pro ih nije ekstrahirao automatskom logičkom ekstrakcijom ni za jedan mobilni uređaj, a metoda koja je usmjerena na ekstrakciju tih podataka je *Downgrade*.

Treću kategoriju čine podaci o preglednicima (engl. *Browser*) koja sadrži informacije o svim Internetskim preglednicima koji se koriste na određenom mobilnom uređaju. Preglednici koji se najčešće koriste su *Google Chrome*, *Safari* (za iOS uređaje), *Mozilla Firefox*, i sl. SPF Pro prikazuje Internetske adrese koje su posjećene, kao i riječi koje su pretraživane. Uz to, prikazuju se i povijest pretraživanja i Internetske oznake, što također može biti vrlo važno u istragama.

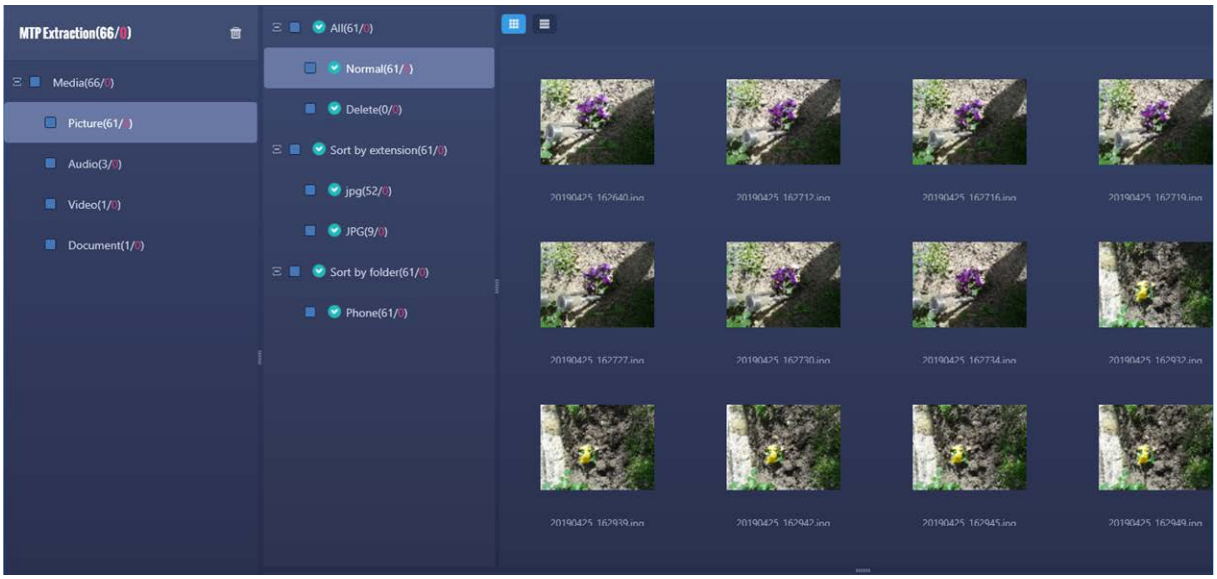
Sljedeća kategorija odnosi se na elektroničku poštu (engl. *E-mail*) te prikazuje sve servise za slanje i primanje elektroničke pošte. Najčešće korišten servis za odvijanje komunikacije putem elektroničke pošte je *Gmail*. SPF Pro prikazuje elektroničku poštu samo za uređaj Samsung Galaxy S3 Mini s ostvarenim *Root* pristupom, a informacije koje su dostupne su adresa elektroničke pošte pošiljatelja i primatelja, tekst elektroničke pošte, datum slanja / primanja elektroničke pošte te način zaštite.

Peta kategorija može se smatrati i najvažnijom jer sadrži medijske zapise (engl. *Media*) koji u većini forenzičkih istraga nose najveću težinu. Svi medijski zapisi analiziraju se na jednak način. SPF Pro ima mogućnost ekstrahiranja izbrisanih medijskih sadržaja što mu dodaje jednu prednost. Sadržaji koji se ekstrahiraju automatskom logičkom ekstrakcijom su slike, audio, video i dokumenti. Ti izvori podataka ekstrahiraju se i MTP ekstrakcijom, a način pregledavanja tih fotografija jednak je za sve uređaje.

Zadnju kategoriju čine fragmentirani podaci. To su podaci koji na neučinkovit način zauzimaju prostor za pohranu. SPF Pro prikazuje njihov broj, kao i broj tih podataka koji su izbrisani u cilju poboljšanja rada mobilnog uređaja. Ti podaci rijetko mogu biti od koristi za forenzičke istrage no forenzički alat SPF Pro ih prikazuje.

6.1.1.2. Obrada podataka ekstrahiranih MTP ekstrakcijom

Obrada podataka ekstrahiranih MTP ekstrakcijom uključuje samo medijske sadržaje. Analiza i obrada ovih podataka jednostavnija je i traje kraće u odnosu na automatsku logičku ekstrakciju. Način na koji se analiziraju podaci ekstrahirani MTP ekstrakcijom nalazi se na sljedećoj slici.



Slika 25: Obrada podataka ekstrahiranih MTP ekstrakcijom

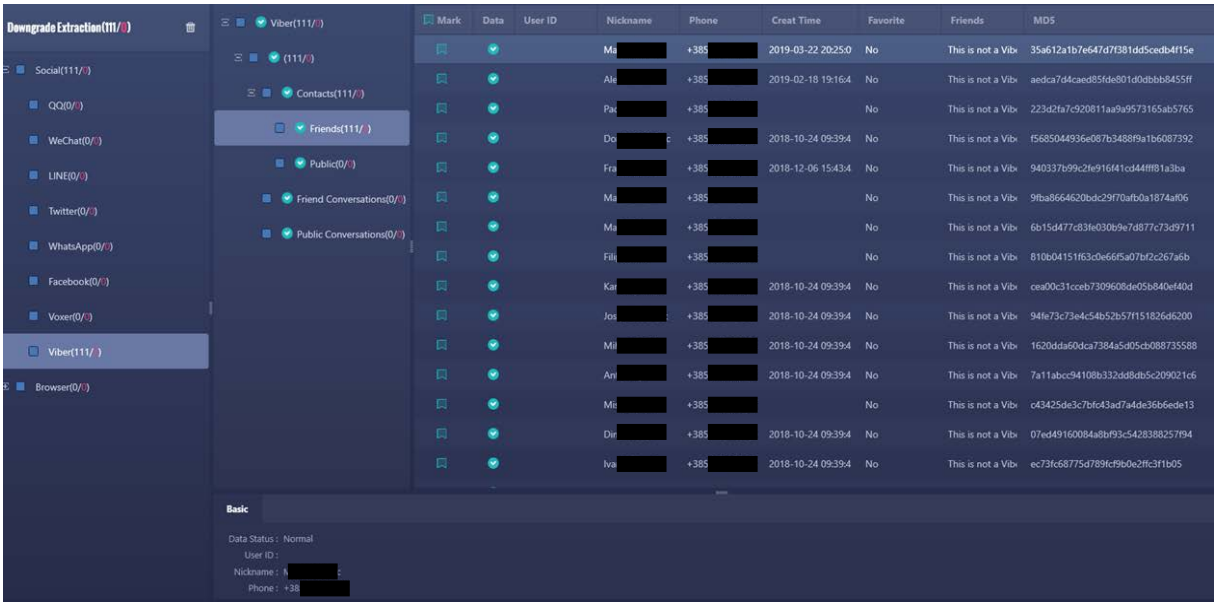
Slika 25 prikazuje način analize ekstrahiranih podataka MTP ekstrakcijom, koji se odvija na istom sučelju za sve ekstrakcije podataka. Iz tog razloga postupak analize jednak je automatskoj logičkoj ekstrakciji, samo su u ovom slučaju ekstrahirani različiti podaci.

Kao što je navedeno, ekstrahiraju se samo medijski sadržaji, a to su:

- **Slike** (engl. *Picture*) – Način analize slika prikazan je na slici 25, a vidljivo je da je analiza jednostavna. Moguće je izvršiti analizu odnosno pretraživanje slika prema nastavku, datoteci u kojoj se nalazi ili prema tome traže li se izbrisane ili neizbrisane slike. Odabir određene slike daje prikaz njenih osnovnih informacija kao što su datum i vrijeme nastanka, naziv slike, veličina te druge osnovne informacije.
- **Zvukovi** (engl. *Audio*) – Analiziraju se na isti način kao i slike te ih je moguće analizirati i pretražiti prema istim elementima. Jedina razlika odnosi se na mogućnost pokretanja određenog zvučnog sadržaja. Također prikazuju se informacije o trajanju zvučnog sadržaja.
- **Videozapisi** (engl. *Video*) – Analiziraju se jednako kao i slike i zvukovi te ih je moguće pokrenuti.
- **Dokumenti** (engl. *Documents*) – Analiza i pretraga dokumenata jednaka je ostalim medijskim zapisima te sadrži jednake mogućnosti pretrage.

6.1.1.3. Obrada podataka ekstrahiranih Downgrade ekstrakcijom

U prethodnom poglavlju navedena je ključna značajka *Downgrade* ekstrakcije, a to je spuštanje aplikacije na nižu verziju. Ova metoda ekstrakcije usmjerena je društvenim mrežama te platformama za komunikaciju. Bila je dostupna samo za uređaj Samsung Galaxy A5, a njome nije ekstrahirana velika količina podataka. Naprotiv, ekstrahirani su samo određeni podaci o *Viber* aplikaciji. Način obrade podataka ekstrahiranih *Downgrade* ekstrakcijom prikazan je na sljedećoj slici, a nazivi i brojevi određenih *Viber* kontakata su prikriveni radi očuvanja privatnosti.



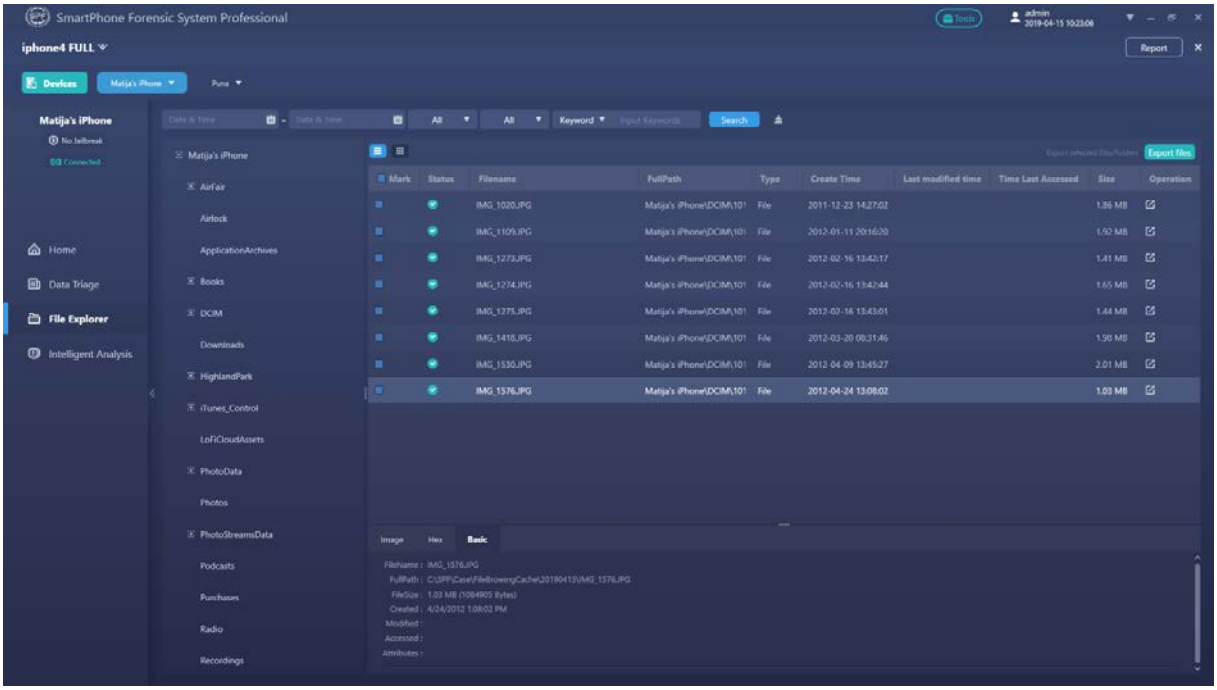
Slika 26: Obrada podataka Downgrade ekstrakcijom

Slika 26 prikazuje sučelje kojim se obrađuju podaci ekstrahirani *Downgrade* ekstrakcijom, a vidljivo je da se izvori podataka odnose isključivo na društvene mreže i platforme za komuniciranje. Alat SPF Pro omogućio je ovu metodu samo na navedenom uređaju, a količina ekstrahiranih podataka je jako mala što je također još jedan nedostatak alata. Način pretraživanja ekstrahiranih podataka vrlo je sličan kao i za ostale podatke ekstrahirane različitim metodama.

6.1.2. Preglednik datoteka

Preglednik datoteka (engl. *File* Explorer) najjednostavniji je način pregledavanja podataka unutar uređaja. Ovaj način također je dostupan za sve obrađene mobilne uređaje, no to ne čudi jer preglednik datoteka ne prikazuje ekstrahirane podatke već samo one koji se nalaze u uređaju, a dokaz tomu je da se preglednik datoteka može primijeniti i prije same ekstrakcije. Može se poistovjetiti s ručnom ekstrakcijom gdje se uz pomoć alata SPF Pro

pregledavaju datoteke u uređaju. Kroz ovu vrstu analize ekstrahiranih podataka moguće je vidjeti strukturu mobilnog uređaja.

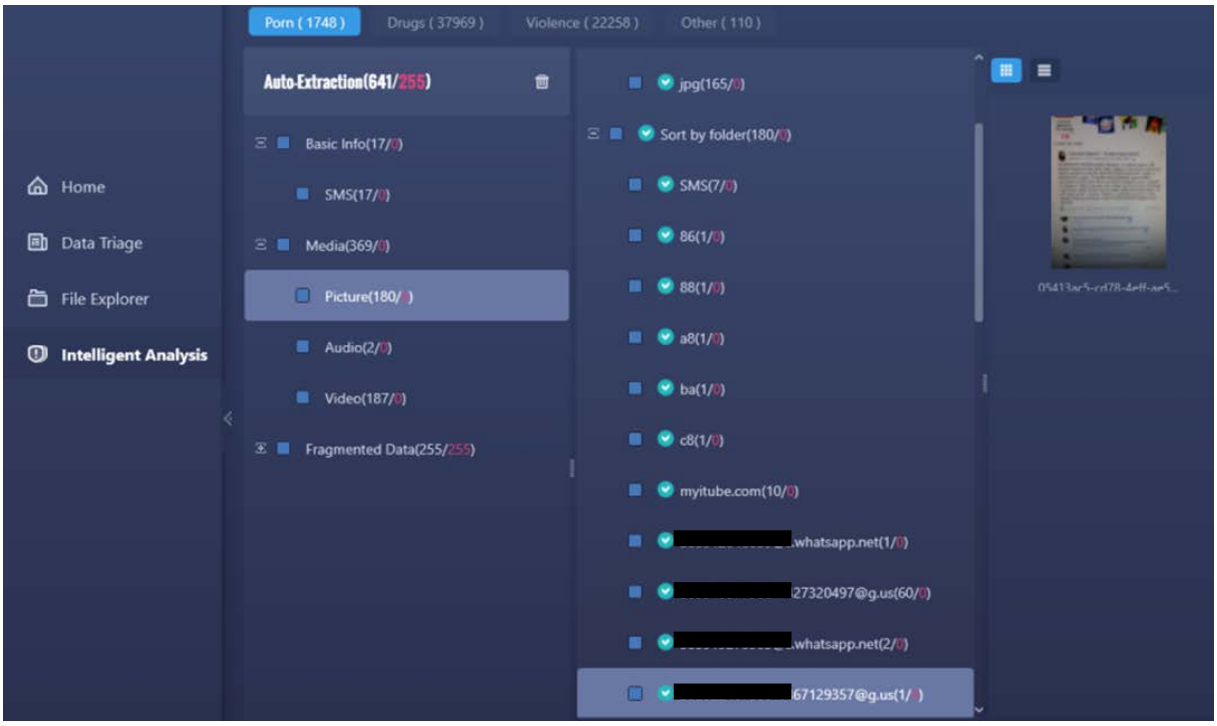


Slika 27: Preglednik datoteka mobilnog uređaja

Slika 27 prikazuje način na koji se pregledavaju datoteke mobilnog uređaja. Ovom vrstom analize moguće je pronaći sve podatke koji su pohranjeni u mobilnom uređaju. Nemoguće je pronaći izbrisane podatke jer je ova metoda usmjerena analizi strukture mobilnog uređaja. Također, moguće je pronaći i medijske zapise no nije ih moguće otvoriti. Ovom vrstom analize nije moguće utvrditi činjenice koje mogu biti značajne za rješavanje određenog slučaja. Jedina prednost ove vrste analize je mogućnost pregledavanja strukture uređaja odmah nakon njegovog povezivanja (bez potrebe za provođenjem ekstrakcije).

6.1.3. Pametno pretraživanje

Pametno pretraživanje (engl. *Intelligent* Analysis) usmjereno je pronalasku zlonamjernih sadržaja na raznim medijskim zapisima. Pretražuje slike, videozapise te i ostale medijske sadržaje te upozorava korisnika na moguće osjetljive sadržaje koji su klasificirani prema pornografiji, nasilju i drogi. Provodi se nakon izvršene ekstrakcije i nije raspoloživa za sve mobilne uređaje. Ovaj algoritam ne radi na ispravan način jer u nekim slučajevima prepoznaje određene slike kao osjetljive sadržaje, no one to nisu, a to će biti prikazano u nastavku.



Slika 28: Pametno pretraživanje mobilnih uređaja

Slika 28 prikazuje način na koji se provodi pametno pretraživanje. Ono je usmjereno na SMS poruke, medijske sadržaje i fragmentirane podatke. Može analizirati i izbrisane ekstrahirane sadržaje, no ovaj način analize podataka ne radi na ispravan način. Analizira osjetljive sadržaje koji sadržavaju elemente pornografije, droge ili nasilja. Na slici je vidljivo da je prikazano 180 slika koje sadrže elemente pornografije, što nije ispravno, jer niti jedna ekstrahirana ne sadrži elemente pornografije. Dakle algoritam ne radi ispravno jer prikazuje prevelik broj osjetljivih sadržaja. To predstavlja veliki nedostatak alatu SPF Pro jer je ovaj način analize podataka beskoristan. Podaci koji su prikriveni na slici 28 odnose se na telefonske brojeve.

6.2. Analiza ekstrahiranih podataka za pojedini mobilni uređaj

Kako je forenzička analiza bila prikazana za pojedini mobilni uređaj, tako će ovo poglavlje prikazati količinu ekstrahiranih podataka za pojedini mobilni uređaj te razlike u podacima koji su ekstrahirani. Ekstrahirani podaci bit će prikazani u tablicama za pojedini mobilni uređaj, a tablice će sadržavati izvore podataka koje alat SPF Pro ekstrahira te metode ekstrakcije podataka koje su ekstrahirali određene podatke.

Tablica prikazuje ekstrahirane podatke u sljedećem obliku:

- X – Ekstrahirani su podaci
- X (x) – Ekstrahirani su podaci uključujući i izbrisane podatke

6.2.1. Analiza ekstrahiranih podataka za uređaj Samsung Galaxy S3 Mini

Forenzička analiza uređaja Samsung Galaxy S3 Mini provedena je za *Root*-ani navedeni uređaj i za uređaj koji nema ostvaren *Root* pristup. Razlike u provođenju forenzičke analize između ova dva uređaja prikazane su u prethodnom poglavlju, a u nastavku će biti prikazane razlike u količini ekstrahiranih podataka.

6.2.1.1. Samsung Galaxy S3 Mini bez ostvarenog Root pristupa

Ovaj mobilni uređaj nema ostvaren *Root* status pa je na njemu bilo moguće provesti samo dvije metode ekstrakcije podataka. Provedba ekstrakcije podataka ovog mobilnog uređaja opisana je u prethodnom poglavlju. Metode kojima su podaci ekstrahirani iz mobilnog uređaja Samsung Galaxy S3 Mini su:

- Automatska logička ekstrakcija
- MTP ekstrakcija

Tablica 2: Analiza ekstrahiranih podataka za uređaj Samsung Galaxy S3 Mini bez ostvarenog *Root* pristupa

Samsung S3 Mini bez *Root* pristupa	Automatska logička ekstrakcija	MTP ekstrakcija
Bluetooth		
Dokumenti		X
Društveni sadržaji		
E-pošta		
Fragmentirani podaci		
Informacije o uređaju	X	
Instalirane aplikacije	X	
Internetski preglednici	X	
Kalendar	X	
Karte		
Kontakti	X	
MMS		
Sat		
Slike		X
SMS	X	
Videozapisi		X
Wi-Fi		
Zapisi poziva	X	
Zvukovi		X

Tablica 2 prikazuje koji su podaci mobilnog uređaja Samsung Galaxy S3 Mini ekstrahirani. Vidljivo je da alat SPF Pro kroz automatsku logičku i MTP ekstrakciju nije ekstrahirao značajnu količinu podataka. Iz ekstrahiranih podataka moguće je zaključiti određene aktivnosti pojedinca, no za rješavanje konkretnog forenzičkog slučaja ekstrahiranih podataka je malo. Automatskom logičkom ekstrakcijom ekstrahirani su osnovni podaci o uređaju, a izvori podataka koji bi mogli dovesti do određenih zaključaka su podaci internetskih preglednika u kojima su vidljive Internetske stranice koje su posjećene s ovog uređaja. Također, ekstrahirani su i SMS-ovi i zapisi poziva, no nisu izbrisani što predstavlja nedostatak. MTP ekstrakcijom ekstrahirani su medijski zapisi koji se nalaze u mobilnom uređaju. Moguće ih je pregledati grafičkim sučeljem, no nisu ekstrahirani izbrisani zapisi. Veliki nedostatak predstavlja nemogućnost ekstrakcije izbrisanih podataka jer će počinitelj određenog kaznenog djela u većini slučajeva izbrisati medijske zapise ili SMS-ove koji mogu dovesti forenzičkog istražitelja do određenog zaključka. Može se zaključiti da provedba forenzičke analize nad ovim uređajem ne daje veliku količinu podataka, a razlog je što mobilni uređaj Samsung Galaxy S3 Mini nije *Root*-an.

6.2.1.2. Samsung Galaxy S3 Mini s ostvarenim Root pristupom

Ovaj uređaj je *Root*-an i iz tog razloga ima mogućnost provođenja jedne metode više u odnosu na uređaj bez *Root* pristupa. Važnost *Root* statusa tijekom postupka ekstrakcije podataka prikazana je u prethodnom poglavlju, a u nastavku slijedi tablica koja će prikazati razliku u ekstrahiranim podacima za iste izvore podataka. Metode ekstrakcije koje su korištene za ekstrahiranje podataka ovog uređaja su:

- Automatska logička ekstrakcija
- Fizička ekstrakcija
- MTP Ekstrakcija

Postupak provođenje fizičke ekstrakcije prikazan je u prethodnom poglavlju, a ona se izvodi na način da kreira forenzičku sliku mobilnog uređaja, a zatim se na toj slici izvode Automatska logička ili MTP ekstrakcija. Podaci koji se nalaze u tablici, a odnose se na fizičku ekstrakciju dobiveni su sumiranjem te dvije ekstrakcije, odnosno sumiranjem količine ekstrahiranih podataka obje metode. Izvori podataka jednaki su kao u prethodnoj tablici.

Tablica 3: Analiza ekstrahiranih podataka za uređaj Samsung Galaxy S3 Mini s ostvarenim *Root* pristupom

Samsung S3 Mini s ostvarenim *Root* pristupom	Automatska logička ekstrakcija	MTP ekstrakcija	Fizička ekstrakcija
Bluetooth			X
Dokumenti	X	X	X (x)
Društveni sadržaji			
E-pošta	X		X

Fragmentirani podaci	X (x)		X (x)
Informacije o uređaju	X		X
Instalirane aplikacije	X		X
Internetski preglednici	X (x)		X (x)
Kalendar	X		X
Karte			
Kontakti	X		X
MMS			
Sat			
Slike	X	X	X (x)
SMS	X (x)		X (x)
Videozapisi	X	X	X (x)
Wi-Fi	X		X
Zapisi poziva	X		X
Zvukovi	X	X	X (x)

Ova tablica prikazuje značajno veću količinu ekstrahiranih podataka u odnosu na prethodnu tablicu. Radi se identičnom uređaju kao i u prethodnoj tablici, no ovaj uređaj ima ostvaren *Root* pristup što omogućava brojne prednosti prilikom ekstrakcije, a što je već nekoliko puta navedeno u radu. Za ovaj uređaj ekstrahirani su svi podaci kao i za prethodni, a veliku prednost za ovaj uređaj donose ekstrahirani izbrisani podaci. Automatskom logičkom ekstrakcijom ekstrahirani su izbrisani podaci Internetskih preglednika i SMS-ova. Podaci Internetskih preglednika prikazuju izbrisane Internetske stranice koje su posjećene, a to se odnosi na stranice koje su izbrisane iz Internetske povijesti. Grafičko sučelje prikazuje SMS poruke te naznačuje one poruke koje su izbrisane, a navedeni izbrisani podaci mogu biti od velike koristi za forenzičke istrage jer se njima može utvrditi potencijalna namjera određenog počinitelja kaznenog djela. Prednost automatske logičke ekstrakcije je ekstrakcija određenih medijskih zapisa i poruka e-pošte što nije bio slučaj za prethodni mobilni uređaj. Druga metoda ekstrakcije koja se primijenila na ovaj uređaj je MTP ekstrakcija, a ona je ekstrahirala identične podatke kao i za prošli mobilni uređaj te također nije uključila izbrisane medijske zapise. Fizička ekstrakcija ekstrahirala je najveću količinu izbrisanih podataka što dovodi do zaključka da je najbolji izbor za ekstrakciju podataka s ovog mobilnog uređaja. Svi podaci koji su ekstrahirani automatskom logičkom ekstrakcijom, ekstrahirani su i fizičkom ekstrakcijom. Prednost fizičkoj ekstrakciji daje mogućnost ekstrahiranja izbrisanih medijskih zapisa, no problem predstavlja njihova analiza jer ih nije moguće otvoriti / pokrenuti u sklopu forenzičkog alata SPF Pro. Fizičkom ekstrakcijom ekstrahirana je veća količina medijskih zapisa nego automatskom logičkom ekstrakcijom, odnosno automatskom logičkom ekstrakcijom nisu ekstrahirani svi medijski zapisi ovog mobilnog uređaja. Analiza podataka ovog uređaja dovodi do zaključka da je ovaj uređaj znatno veći izvor korisnih podataka u odnosu na uređaj koji nije *Root*-an, a najznačajniji podaci ekstrahirani su fizičkom ekstrakcijom.

6.2.2. Analiza ekstrahiranih podataka za uređaj Samsung Galaxy A5

Sljedeća tablica prikazuje količinu ekstrahiranih podataka za mobilni uređaj Samsung Galaxy A5 koji ima najnoviju verziju operativnog sustava među uređajima obrađenim u ovom radu. Postupak ekstrakcije podataka vidljiv je u prethodnom poglavlju, a sljedeća tablica će prikazati što se pojedinom metodom ekstrahiralo. SPF Pro omogućava provedbu sljedećih metoda ekstrakcije nad ovim uređajem:

- Automatska logička ekstrakcija
- Downgrade ekstrakcija
- MTP ekstrakcija

Tablica 4: Analiza ekstrahiranih podataka za uređaj Samsung Galaxy A5

Samsung Galaxy A5	Automatska logička ekstrakcija	MTP ekstrakcija	Downgrade ekstrakcija
Bluetooth			
Dokumenti		X	
Društveni sadržaji			X
E-pošta			
Fragmentirani podaci			
Informacije o uređaju	X		
Instalirane aplikacije	X		
Internetski preglednici			
Kalendar	X		
Karte			
Kontakti			
MMS			
Sat			
Slike		X	
SMS			
Videozapisi		X	
Wi-Fi			
Zapisi poziva			
Zvukovi		X	

Samsung Galaxy A5 uređaj je novijeg datuma i sadrži novije i poboljšanije sustave zaštite u odnosu na starije uređaje. To se odražava na količinu ekstrahiranih podataka što je vidljivo u tablici 4. Automatskom logičkom ekstrakcijom ekstrahirani su samo podaci o uređaju, instaliranim aplikacijama te kalendaru. Iz tih podataka nemoguće je donijeti zaključak o ponašanju korisnika tog uređaja što alatu SPF Pro donosi još jedan nedostatak. Također, vidljivo je da automatskom logičkom, MTP i *Downgrade* ekstrakcijom nije ekstrahiran niti jedan izbrisani podatak što je također veliki nedostatak. MTP ekstrakcija

ekstrahirala je sve medijske zapise koji se nalaze u uređaju, no to se ne može smatrati kao prednost jer je to moguće izvesti i najjednostavnijom ručnom ekstrakcijom. *Downgrade* ekstrakcija usmjerena je društvenim mrežama i platformama za komunikaciju, no za ovaj uređaj ekstrahirala je samo kontakte *Viber* aplikacije. Nije ekstrahirana ni jedna poruka, prenesena fotografija ili slično. Pogledom na tablicu 4 moguće je zaključiti da forenzički alat SPF Pro nije dobro rješenje za ekstrakciju podataka s ovog uređaja jer se ne ekstrahira ni jedan značajni podatak.

6.2.3. Analiza ekstrahiranih podataka za uređaj HTC Desire 610

HTC Desire 610 još je jedan Android uređaj koji je korišten za izradu diplomskog rada. Kao što je objašnjeno u prethodnom poglavlju, ekstrakcija ovog uređaja gotovo je jednaka kao i za Samsung Galaxy S3 Mini bez ostvarenog *Root* pristupa. Količina ekstrahiranih podataka prikazana je u tablici 5, a metode koje su korištene za ekstrakciju podataka su:

- Automatska logička ekstrakcija
- MTP ekstrakcija

Tablica 5: Analiza ekstrahiranih podataka za uređaj HTC Desire 610

HTC Desire 610	Automatska logička ekstrakcija	MTP ekstrakcija
Bluetooth		
Dokumenti	X	
Društveni sadržaji		
E-pošta		
Fragmentirani podaci		
Informacije o uređaju	X	
Instalirane aplikacije	X	
Internetski preglednici	X	
Kalendar	X (x)	
Karte		
Kontakti	X	
MMS		
Sat		
Slike	X	
SMS	X	
Videozapisi	X	
Wi-Fi		
Zapisi poziva	X	
Zvukovi	X	

Tablica 5 razlikuje se od ostalih jer MTP ekstrakcija nije ekstrahirala nikakve medijske sadržaje. Postupak ekstrakcije uspješno je završio, no analizom nije bilo moguće utvrditi nikakve ekstrahirane podatke, što je nedostatak SPF Pro alata u ekstrakciji podataka s ovog uređaja. Automatska logička ekstrakcija ekstrahirala je osnovne podatke o uređaju te medijske zapise. Jedini izbrisani podaci koji su ekstrahirani su podaci kalendara, što u nekim slučajevima može predstavljati koristan izvor informacija, no bez drugih izbrisanih podataka teško je nešto zaključiti. Prednost predstavlja ekstrakcija SMS poruka, zapisa poziva i Internetskih preglednika, no oni također nisu izbrisani. Ekstrahirani su svi medijski zapisi na uređaju, međutim ponovno bez onih izbrisanih. Može se zaključiti da forenzički alat SPF Pro nije dobro rješenje za ovaj uređaj jer MTP ekstrakcija nema nikakve koristi, a automatska logička ekstrakcija ne ekstrahira značajne izbrisane podatke.

6.2.4. Analiza ekstrahiranih podataka za uređaj iPhone 4

Sljedeća tablica prikazat će količinu ekstrahiranih podataka za mobilni uređaj koji radi na iOS operativnom sustavu. U poglavlju 5 opisane su metode koje se koriste za ekstrakciju podataka mobilnog uređaja iPhone 4, a te iste metode bit će prikazane u sljedećoj tablici. Ovaj mobilni uređaj analiziran je i obrađen brojnim alatima te je upravo on uređaj iz kojega se ekstrahira najveća količina značajnih podataka, a to će biti prikazano na tablici 6. Tablica će dati odgovor je li takvo stanje u alatu SPF Pro. Metode koje su omogućene za ovaj uređaj su:

- Automatska logička ekstrakcija
- Datotečna ekstrakcija
- MTP ekstrakcija

Fizička ekstrakcija uređaja Samsung Galaxy S3 Mini provodila se na način da se prvo kreirala forenzička slika, a zatim se ta slika obrađivala automatskom logičkom i MTP ekstrakcijom. Na isti način se provodi datotečna ekstrakcija, a podaci koji se nalaze u tablici dobiveni automatskom logičkom ekstrakcijom jer je MTP ekstrakcija podržana samo za Android uređaje.

Tablica 6: Analiza ekstrahiranih podataka za uređaj iPhone 4

iPhone 4	Automatska logička ekstrakcija	MTP ekstrakcija	Datotečna ekstrakcija
Bilješke			X (x)
Bluetooth	X		X
Dokumenti			X
Društveni sadržaji			
E-pošta			
Fragmentirani podaci			X (x)
Informacije o uređaju	X		X
Instalirane aplikacije	X		X

Internetski preglednici			X
Kalendar			X (x)
Karte			
Kontakti			X
Korisnički računi			X
MMS			X
Sat			
Slike		X	X
SMS			X (x)
Videozapisi		X	X
Wi-Fi	X		X
Zapisi poziva			X (x)
Zvukovi			X

Analizom uređaja iPhone 4 mogu se pregledati podaci koji mogu biti korisni u forenzičkim istragama jer alat SPF Pro ekstrahira veliku količinu značajnih podataka. Ova tablica sadrži dodatna dva izvora podataka koji se ekstrahiraju samo za iOS uređaje, a to su bilješke i korisnički računi. Automatska logička ekstrakcija ekstrahirala je vrlo malo korisnih podataka, a jedini podaci koji mogu biti korisni su oni o Wi-Fi mrežama na koje je mobilni uređaj bio povezan. Iz tih podataka moguće je utvrditi datum, vrijeme i lokaciju na kojoj se mobilni uređaj nalazio. MTP ekstrakcija ekstrahirala je podatke na drugačiji način nego li je to bio slučaj za prethodne mobilne uređaje jer nije ekstrahirala dokumente i zvukove. Ekstrahirala je određene slike i videozapise iz mobilnog uređaja, ali nije sve. Također, nedostatak je što automatskom logičkom i MTP ekstrakcijom nije ekstrahiran ni jedan izbrisani podatak. Datotečna ekstrakcija ovog uređaja ekstrahirala je veliku količinu značajnih i izbrisanih podataka. Velika prednost datotečne ekstrakcije u odnosu na prethodne dvije metode je ekstrakcija izbrisanih SMS poruka, zapisa poziva, podataka kalendara i bilješki. Datotečna ekstrakcija ekstrahirala je sve medijske zapise, uključujući zvukove i dokumente, no njen nedostatak je što nije ekstrahirala izbrisane. Analizom i sumiranjem svih podataka koji su ekstrahirani za ovaj uređaj dolazi se do zaključka da je alat SPF Pro zadovoljavajuć i da se njime mogu ekstrahirati značajni podaci za forenzičke istrage. Automatska logička i MTP ekstrakcija gotovo su nepotrebne jer Datotečna ekstrakcija ekstrahira puno više značajnih podataka.

6.3. Validacija količine ekstrahiranih podataka alata SPF Pro u odnosu na druge alate iste namjene

Tablica 1 prikazala je usporedbu mogućnosti alata SPF Pro u odnosu na druge alate iste namjene, a tablice koje slijede prikazat će usporedbu količine ekstrahiranih podataka u odnosu na druge alate iste namjene. Za potrebe izrade sljedećih tablica korišteni su brojni alati te su provedene sve dostupne ekstrakcije podataka, a krajnji rezultat koji se nalazi u tablicama

dobiven je sumiranjem svih ekstrahiranih podataka iz različitih metoda ekstrakcije. Na primjer, za pojedini alat logičkom ekstrakcijom ekstrahirale su se poruke, a datotečnom ekstrakcijom izbrisane poruke, taj rezultat se povezao i došlo se do zaključka da se određenim alatom mogu ekstrahirati izbrisane poruke neovisno o kojoj se metodi radi. Svi mobilni uređaji koji su korišteni za izradu diplomskog rada analizirani su kroz brojne alate, a što će biti vidljivo na idućim tablicama.

Tablice će biti popunjene na sljedeći način:

- X – Ekstrahirani su podaci
- X (x) – Ekstrahirani su podaci uključujući i izbrisane podatke

6.3.1. Samsung Galaxy S3 Mini

6.3.1.1. Samsung Galaxy S3 Mini bez ostvarenog Root pristupa

Tablica 7: Usporedni prikaz ekstrahiranih podataka korištenjem brojnih alata za mobilni uređaj Samsung Galaxy S3 Mini bez ostvarenog *Root* pristupa

Samsung S3 Mini bez *Root* pristupa	Belkasoft Acqustion	Oxygen	**SPF Pro**	UFED Touch 2
Aplikacije				
Viber				
Facebook				
WhatsApp				
Skype				
iMessage				
Instagram				
Audio			X	X
Baze podataka				X
Bilješke				
Bluetooth				
Dokumenti	X		X	
E-mail poruke				
Fotografije	X		X	X
Instalirane aplikacije	X		X	X (x)
Kalendar			X	
Kolačići				X (x)
Konfiguracija				
Kontakti	X	X	X	X (x)
Korisnički računi				X
Lokacije				
Lozinke				X
O uređaju		X	X	X
plist				
Popis poziva	X		X	

Povijest web pretraživanja			X	
Pretraživanja				X
SMS			X	
Upotreba aplikacija				
Video	X		X	X
Web oznake				X (x)
Wi-Fi				X

Na tablici 7 vidljivo je da je hardverski alat UFED Touch 2 bolje rješenje nego SPF Pro za uređaj Samsung Galaxy S3 Mini jer je ekstrahirao puno veću količinu podataka, a za određene elemente uspio je ekstrahirati i izbrisane sadržaje. Iako je alat SPF Pro lošiji izbor u odnosu na „UFED Touch 2“ za navedeni uređaj, bolje je rješenje nego alati „Belkasoft Acquisition Tool“ i „Oxygen Forensics“.

6.3.1.2. Samsung Galaxy S3 Mini s ostvarenim Root pristupom

Tablica 8: Usporedni prikaz ekstrahiranih podataka korištenjem brojnih alata za mobilni uređaj Samsung Galaxy S3 Mini s ostvarenim *Root* pristupom

Samsung Galaxy S3 Mini s *Root* pristupom	Belkasoft Acqustion	Oxygen	**SPF Pro**	UFED Touch 2
Aplikacije				
Viber				
Facebook				
WhatsApp				
Skype				
iMessage				
Instagram				
Audio		X (x)	X	X
Baze podataka		X (x)		X
Bilješke		X		
Bluetooth			X	
Dokumenti	X		X (x)	
E-mail poruke		X (x)	X	X (x)
Fotografije	X	X (x)	X (x)	X
Instalirane aplikacije	X	X	X	X (x)
Kalendar		X	X	
Kolačići	X			X
Konfiguracija				X
Kontakti	X	X (x)	X	X (x)
Korisnički računi		X	X	X
Lokacije		X (x)		
Lozinke	X	X	X	X
O uređaju		X	X	X

Plist				
Popis poziva	X		X	
Povijest web pretraživanja	X	X	X (x)	X (x)
Pretraživanja				X
SMS			X (x)	
Upotreba aplikacija				X (x)
Video	X	X (x)	X	X
Web oznake		X	X (x)	X (x)
Wi-Fi		X	X	X

Tablica 8 prikazuje da je za *Root*-ani uređaj Samsung Galaxy S3 Mini alat SPF Pro dobro rješenje jer je ekstrahirao veliku količinu podataka uključujući i izbrisane podatke. U odnosu na „Belkasoft Acquisition Tool“ predstavlja bolji alat, a za ovaj uređaj može parirati alatima „Oxygen Forensics“ i „UFED Touch 2“. Kao ni za Samsung Galaxy S3 Mini koji nema ostvaren *Root* pristup ni kod ovog uređaja se nisu ekstrahirali podaci društvenih mreža i platformi za komunikaciju. Vidljivo je da na sve alate isključujući „Belkasoft Acquisition Tool“ utječe *Root* status uređaja.

6.3.2. Samsung Galaxy A5

Tablica 9: Usporedni prikaz ekstrahiranih podataka korištenjem brojnih alata za mobilni uređaj Samsung Galaxy A5

Samsung Galaxy A5		Belkasoft Acqustion	Oxygen	**SPF Pro**	UFED Touch 2
Aplikacije					
	Viber			X	
	Facebook				
	WhatsApp				
	Skype				
	iMessage				
	Instagram				
Audio			X	X	X
Baze podataka			X		X
Bilješke					
Bluetooth					
Dokumenti		X	X	X	X
E-mail poruke					
Fotografije		X	X	X	X
Instalirane aplikacije			X	X	X
Kalendar		X	X	X	X
Kolačići					X
Konfiguracija					X
Kontakti			X		X

Korisnički računi	X	X		X
Lokacije				
Lozinke				
O uređaju		X	X	X
Plist				
Popis poziva		X		X
Povijest web pretraživanja	X			
Pretraživanja				
SMS		X		X
Upotreba aplikacija				
Video	X	X	X	X
Web oznake				
Wi-Fi				

Ova tablica prikazuje količinu ekstrahiranih podataka za mobilni uređaj Samsung Galaxy A5 koji nema ostvaren *Root* pristup. Vidljivo je da niti jedan alat nije ekstrahirao izbrisane podatke, a razlog tomu je što mobilni uređaj radi na Android verziji 8.0.0. i što je novijeg datuma pa su sigurnosni mehanizmi značajno čvršći nego li je to slučaj u ostalim obrađenim mobilnim uređajima. Najveću količinu podataka ekstrahirao je alat „UFED Touch 2“, no alat SPF Pro ima jednu veliku prednost što se tiče ovog mobilnog uređaja, a to je da je ekstrahirao poruke iz „Viber“ platforme za komunikaciju.

6.3.3. HTC Desire 610

Tablica 10: Usporedni prikaz ekstrahiranih podataka korištenjem brojnih alata za mobilni uređaj HTC Desire 610

HTC Desire 610		Belkasoft Acqustion	Oxygen	**SPF Pro**	UFED Touch 2
Aplikacije					
	Viber				
	Facebook	X	X (x)		
	WhatsApp		X (x)		
	Skype				
	iMessage				
	Instagram		X (x)		
Audio			X	X	X
Baze podataka			X		X (x)
Bilješke					
Bluetooth					
Dokumenti		X	X	X	X
E-mail poruke			X		X (x)
Fotografije		X	X	X	X (x)
Instalirane aplikacije		X	X	X	X (x)

Kalendar	X	X	X (x)	X (x)
Kolačići	X	X (x)		X (x)
Konfiguracija				X
Kontakti	X	X (x)	X	X (x)
Korisnički računi		X		X
Lokacije	X	X (x)		X
Lozinke		X		X (x)
O uređaju		X	X	X
Plist				
Popis poziva	X	X (x)	X	X (x)
Povijest web pretraživanja	X			X (x)
Pretraživanja				
SMS		X (x)	X	X (x)
Upotreba aplikacija				
Video	X	X	X	X
Web oznake				
Wi-Fi		X		X

Forenzički alat SPF Pro predstavlja loše rješenje za ekstrakciju podataka mobilnog uređaja HTC Desire 610. To se može zaključiti pogledom na tablicu 10 na kojoj je vidljivo da „UFED Touch 2“ i „Oxygen Forensics“ ekstrahiraju znatno veću količinu podataka. Također, nedostatak SPF Pro alata u ovom slučaju je što ne ekstrahira podatke društvenih mreža niti platformi za komunikaciju, a što navedena dva alata čine. SPF Pro se prikazuje kao dosta nejasan alat jer za svaki drugi uređaj ekstrahira potpuno različitu količinu podataka.

6.3.4. iPhone 4

Tablica 11: Usporedni prikaz ekstrahiranih podataka korištenjem brojnih alata za mobilni uređaj iPhone 4

iPhone 4		Belkasoft Acqustion	Oxygen	**SPF Pro**	UFED Touch 2
Aplikacije			X		X (x)
	Viber	X	X (x)		X (x)
	Facebook		X		
	WhatsApp	X	X (x)		X (x)
	Skype	X	X (x)		X
	iMessage				X (x)
	Instagram		X		
Audio		X	X	X	X
Baze podataka			X		X
Bilješke		X	X	X (x)	X
Bluetooth		X		X	X
Dokumenti		X		X	X

E-mail poruke	X			X (x)
Fotografije	X	X	X	X (x)
Instalirane aplikacije	X	X	X	X
Kalendar	X	X	X (x)	X (x)
Kolačići				X (x)
Konfiguracija	X			X (x)
Kontakti	X	X (x)	X	X (x)
Korisnički računi	X	X	X	X
Lokacije	X	X		X (x)
Lozinke		X		X
O uređaju	X	X	X	X
Plist	X			
Popis poziva	X	X (x)	X (x)	X (x)
Povijest web pretraživanja	X	X	X	X
Pretraživanja				X
SMS	X	X (x)	X (x)	X (x)
Upotreba aplikacija				X
Video	X	X	X	X
Web oznake				X
Wi-Fi	X	X	X	X

iPhone 4 je mobilni uređaj iz kojeg se može ekstrahirati najveća količina podataka. Gotovo svi alati koji se nalaze u tablici 11 ekstrahiraju veliku količinu podataka. Vidljivo je da je „UFED Touch 2“ daleko bolji od ostalih alata jer je ekstrahirao veliku količinu izbrisanih podataka. Razlog zašto je toliko podataka s uređaja iPhone 4 ekstrahirano je njegova verzija operativnog sustava i godina proizvodnje, koja je dosta stara. I u ovom slučaju SPF Pro ne ekstrahira podatke društvenih mreža te platformi za komunikaciju što je dosta veliki nedostatak u odnosu na druge alate.

7. Zaključak

Mobilna forenzika relativno je novo područje u digitalnim tehnologijama te se u budućim godinama očekuje značajni porast u primjeni. Sve više kriminalnih dijela na određeni način uključuje primjenu mobilnih uređaja pa će i iz tog razloga mobilna forenzika biti sve više tražena. Trenutni broj forenzičkih istražitelja nije velik, no očekuje se i njihov porast iz već navedenih razloga. Forenzički istražitelji moraju stalno pratiti trendove mobilne forenzike te se neprestano obučavati kako bi na što lakši način provodili forenzičku analizu mobilnih uređaja.

Mobilni uređaji danas predstavljaju rudnik digitalnih dokaza kojima se mogu riješiti razne forenzičke istrage. Metode ekstrakcije koje su navedene u diplomskom radu najčešće se primjenjuju, ali postoji još mnogo metoda ekstrakcija kojima se pokušavaju ekstrahirati podaci mobilnih uređaja. Današnji noviji mobilni uređaji imaju snažne obrambene sustave, odnosno sustave zaštite pa je u nekim slučajevima ekstrakcija njihovih podataka izrazito komplicirana ili nemoguća. U skorijoj budućnosti može se očekivati razvoj novih metoda ekstrakcija koje će biti usmjerene probijanju sigurnosnih mehanizama takvih uređaja.

Forenzički alat SPF Pro predstavlja se kao moćan softverski alat digitalne forenzike. Iz diplomskog rada se može zaključiti da praksa dokazuje nešto drugo. Sučelje i način upravljanja alatom su vrlo jednostavni i lako razumljivi, a alat na dobar način prepoznaje povezane mobilne uređaje. Postupak ekstrakcije podataka za određenu metodu uglavnom je jednak te također lako razumljiv. Na mogućnosti alata mogu utjecati brojni čimbenici, a diplomski rad dokazao je da je jedan od čimbenika *Root* status mobilnog uređaja koji omogućuje više metoda ekstrakcije te se ekstrahira veća količina podataka. Na mogućnosti alata također mogu utjecati vrsta operativnog sustava te njegova verzija. Tako se za uređaj iPhone 4 koji radi na iOS operativnom sustavu verzije 7.1 ekstrahira velika količina podataka za razliku od uređaja Samsung Galaxy A5 koji radi na Android operativnom sustavu verzije 8.0.0 gdje se ne ekstrahiraju nikakvi značajni podaci. Prednost alatu daju dodatni alati koji se mogu koristiti za dodatne načine ekstrakcije podataka ili *Root*-anje mobilnih uređaja

Može se zaključiti da forenzički alat SPF Pro ne može konkurirati forenzičkim alatima iste namjene (Oxygen Forensics, UFED Touch 2) jer ne ekstrahira toliku količinu podataka. Nedostatak mu predstavlja pogrešan način rada jedne metode analize podataka, a to je pametno pretraživanje (engl. *Intelligent Analysis*) koja bi trebala dati moć forenzičkom alatu u otkrivanju osjetljivog i nedopuštenog sadržaja. Još jedan nedostatak predstavlja mali broj podržanih ekstrakcija za mobilne uređaje koji su obrađeni u diplomskom radu. U slučaju ovog alata bilo bi vrlo poželjno ostvariti *Root* status ako bi pravila istrage to dozvolila. SPF Pro uglavnom se koristi za brze i jednostavne ekstrakcije podataka mobilnih uređaja.

Literatura

[1] Autorizirana predavanja: *Metodologije digitalne forenzike*, Fakultet prometnih znanosti Izvor:https://moodle.srce.hr/2018-2019/pluginfile.php/1984374/mod_resource/content/3/4_Metodologije%20digitalne%20forenzike_31102018.pdf (pristupljeno: lipanj 2019.)

[2] URL:https://www.techopedia.com/definition/27805/digital-forensics (pristupljeno: lipanj 2019.)

[3] Gogolin, G.: *Digital Forensics Explained*, London, 2012.

[4] Androulidakis, I. I.: *Mobile Phone Security and Forensics: A Practical Approach*, USA, 2014.

[5] Casey, E.: *Digital Forensics and Investigation*, USA, 2009.

[6] Sammons, J.: *The Basics of Digital Forensics*, USA, 2012.

[7] URL:https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A163/datastream/PDF/view (pristupljeno: lipanj 2019.)

[8] Autorizirana predavanja: *Osnove digitalnih dokaza*, Fakultet prometnih znanosti Izvor:https://moodle.srce.hr/2018-2019/pluginfile.php/1984371/mod_resource/content/3/03_Primjena%20digitalne%20forenzike%20i%20digitalni%20dokazi.pdf (pristupljeno: lipanj 2019.)

[9] URL:http://sigurnost.zemris.fer.hr/ostalo/2010_marceta/Diplomski.htm#_Toc261209076 (pristupljeno: lipanj 2019.)

[10] Bommisetty, S., Tamma, R., Mahalik, H.: *Practical Mobile Forensics*, Birmingham, 2012.

[11] URL:https://www.academia.edu/27667604/Osnovne_karakteristike_digitalnih_dokaza (pristupljeno: lipanj 2019.)

[12] URL:http://nevena.lss.hr/recordings/fer/predmeti/racfor/2018/seminari/flozic/seminar.pdf (pristupljeno: lipanj 2019.)

[13] URL:http://gs.statcounter.com/os-market-share/mobile/worldwide (pristupljeno: lipanj 2019.)

[14] Tahiri, S.: *Mastering Mobile Forensics*, Birmingham, 2016.

[15] URL:https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/ (pristupljeno: lipanj 2019.)

[16] Graves, M.W.: *Digital Archaeology*, USA, 2013.

[17] URL:https://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf (pristupljeno: srpanj 2019.)

[18] URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf (pristupljeno: srpanj 2019.)

[19] URL:https://www.gillware.com/digital-forensics/gps-forensics/ (pristupljeno: srpanj 2017.)

[20] URL: https://www.researchgate.net/publication/300715450_New_Technique_of_Forensic_Analysis_for_Digital_Cameras_in_Mobile_Devices (pristupljeno: srpanj 2019.)

[21] URL:http://www.cis.hr/WikiIS/doku.php?id=web_forenzika (pristupljeno: srpanj 2019.)

[22] URL:http://www.forensicswiki.org/wiki/SMS (pristupljeno: srpanj 2019.)

[23] URL:https://www.irjet.net/archives/V3/i7/IRJET-V3I7375.pdf (pristupljeno: srpanj 2019.)

[24] URL: https://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1016&context=electricalcomputerengineering-facpubs (pristupljeno: srpanj 2019.)

[25] URL:http://www.acquireforensics.com/services/data/memory-card.html (pristupljeno: srpanj 2019.)

[26] URL:https://sigurnostnamrezi.wordpress.com/2015/12/08/digitalne-antiforenzicke-tehnike/ (pristupljeno: srpanj 2019.)

[27] Autorizirana predavanja: *Antiforenzika i izvještavanje*, Fakultet prometnih znanosti Izvor: https://moodle.srce.hr/2018-2019/pluginfile.php/2106086/mod_resource/content/0/Antiforenzika%20i%20izvje%C5%A1tavanje.pdf (pristupljeno: srpanj 2019.)

[28] URL:https://lecto-player.lecto.org/recordings/fer/predmeti/racfor/2016/seminari/jspaunjarallah/seminar.pdf (pristupljeno: srpanj 2019.)

[29] URL:https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf (pristupljeno: srpanj 2019.)

[30] URL: https://www.veleri.hr/files/datotekep/nastavni_materijali/k_informatika_1/Uvod_u_kriptografiju.pdf (pristupljeno: srpanj 2019.)

[31] Milanović, Z., Milanović, T.: *Digitalna anti-forenzika kao kriminogeno sredstvo zaštite kiber kriminala*, Beograd, 2010.

[32] URL:https://www.researchgate.net/publication/279175024_Digitalna_antiforenzika-manipulacija_procesom_digitalne_istrage (pristupljeno: srpanj 2019.)

[33] Autorizirana predavanja: *Digitalni dokazi i ekstrakcija podataka mobilnih uređaja*, Fakultet prometnih znanosti
Izvor: https://moodle.srce.hr/2018-2019/pluginfile.php/2103478/mod_resource/content/1/07_Digitalni%20dokazi%20i%20ekstrakcija%20podataka%20mobilnih%20ure%C4%91aja%201.pdf (pristupljeno: srpanj 2019.)

[34] URL:https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf (pristupljeno: srpanj 2019.)

[35] URL: http://www.teeltech.com/wp-content/uploads/2013/10/VDB_InTransport_web.jpg (pristupljeno: srpanj 2019.)

[36] URL:http://ijcsit.com/docs/Volume%206/vol6issue05/ijcsit20150605150.pdf (pristupljeno: srpanj 2019.)

[37] URL:https://www.nist.gov/sites/default/files/documents/forensics/2-Brothers-NIST-2014_Slides-23-Pages-2.pdf (pristupljeno: srpanj 2019.)

[38] URL:https://counterespionage.com/advanced-tscm-explained/data-extraction/ (pristupljeno: srpanj 2019.)

[39] URL:http://blog.specialcounsel.com/ediscovery/three-types-of-mobile-device-extractions-and-what-each-contains/ (pristupljeno: srpanj 2019.)

[40] URL:https://digital-forensics.sans.org/blog/2008/09/03/hex-dumping-flash-from-a-mobile (pristupljeno: srpanj 2019.)

[41] URL:http://www.binaryintel.com/services/jtag-chip-off-forensics/jtag-forensics/ (prsitupljeno: srpanj 2019.)

[42] URL:http://detektiv-mreza.hr/hr/specijalnost/forenzika-mobilnih-uredaja-1 (pristupljeno: srpanj 2019.)

[43] URL:https://digitalna-forenzika.com/napredni-forenzicki-postupci-chip-off/ (pristupljeno: srpanj 2019.)

[44] URL:http://www.binaryintel.com/wp-content/uploads/2013/02/CHIP-OFF_FORENSIC_WATER_DAMAGED_CELL_PHONE.jpg (pristupljeno: srpanj 2019.)

[45] Autorizirana predavanja: *Ekstrakcija podataka i memorijski sustavi*, Fakultet prometnih znanosti
Izvor:https://moodle.srce.hr/2018-2019/pluginfile.php/2103499/mod_resource/content/1/08_Ekstrakcija%20podataka%20i%20memorijski%20sustavi.pdf (pristupljeno: srpanj 2019.)

[46] URL:http://www.teeltech.com/mobile-device-forensics-training/in-system-programming-for-mobile-device-forensics/ (pristupljeno: srpanj 2019.)

[47] URL:http://www.farleyforensics.com/2019/04/10/basic-overview-of-jtag-isp-chipoff-extractions/ (pristupljeno: srpanj 2019.)

[48] URL:http://www.studioag.pro/en/2011/10/le-flasher-box-per-lanalisi-forense-dei-cellulari/ (pristupljeno: srpanj 2019.)

[49] URL:https://www.forensicmag.com/product-release/2010/07/flasher-boxes-back-basics-mobile-phone-forensics (pristupljeno: srpanj 2019.)

[50] URL:https://live.staticflickr.com/2948/15486849525_351c5b4698_b.jpg (pristupljeno: srpanj 2019.)

[51] URL: https://www.researchgate.net/publication/265295989_Forensic_Challenges_in_Mobile_Cloud_Computing (pristupljeno: srpanj 2019.)

[52] URL:https://www.linkedin.com/pulse/forenzi%C4%8Dka-analiza-mobilnih-ure%C4%91aja-miroslav-klarica (pristupljeno: srpanj 2019.)

[53] URL:https://www.linkedin.com/pulse/forenzi%C4%8Dka-analiza-mobilnih-ure%C4%91aja-miroslav-klarica (pristupljeno: srpanj 2019.)

[54] URL:http://www.digital-evidence.org/papers/opensrc_legal.pdf (pristupljeno: kolovoz 2019.)

[55] URL:https://www.csoonline.com/article/2117658/rules-of-evidence---digital-forensics-tools.html (pristupljeno: kolovoz 2019.)

[56] URL:http://www.digital-evidence.org/papers/dfrws_define.pdf (pristupljeno: kolovoz 2019.)

[57] URL:https://www.dhs.gov/sites/default/files/publications/Digital-Forensics-Tools-TN_0716-508.pdf (pristupljeno: kolovoz 2019.)

[58] URL: https://www.ieee.hr/_download/repository/03_Ieee_Uvod_u_racunalnu_forenziku.pdf (pristupljeno: kolovoz 2019.)

[59] URL:http://www.salvationdata.com/about.html (pristupljeno: kolovoz 2019.)

[60] SalvationDATA: *Mobile Forensic SPF Pro Datasheet*, Kina,

[61] SalvationDATA: *Mobile Forensics SPF Pro Feature List*, Kina,

[62] URL:https://mob.hr/sto-je-to-root/ (pristupljeno: kolovoz 2019.)

[63] URL:http://www.droid.hr/tutorial-kako-rootati-android/ (pristupljeno: kolovoz 2019.)

[64] URL:https://fileinfo.com/extension/plist (pristupljeno: kolovoz 2019.)

[65] URL:https://www.w3schools.com/sql/ (pristupljeno: kolovoz 2019.)

[66] URL:https://www.lifewire.com/what-is-md5-2625937 (pristupljeno: kolovoz 2019.)

[67] SalvationDATA: *Mobile Forensic Tool Comparison*, Kina,

[68] URL:https://www.gsmarena.com/samsung_i8190_galaxy_s_iii_mini-5033.php (pristupljeno: kolovoz 2019.)

[69] URL: https://uk.static.webuy.com/product_images/Phones/Phones%20Android/SSAMI81908GBUNLB_l.jpg (pristupljeno: kolovoz 2019.)

[70] URL:https://www.gsmarena.com/samsung_galaxy_a5_(2017)-8494.php (pristupljeno: kolovoz 2019.)

[71] URL:https://images-na.ssl-images-amazon.com/images/I/51roXjeR3qL._SX425_.jpg (pristupljeno: kolovoz 2019.)

[72] URL:https://www.gsmarena.com/htc_desire_610-6160.php (pristupljeno: kolovoz 2019.)

[73] URL:https://static.turbosquid.com/Preview/2014/08/02__04_12_14/1.jpgd7da8b67-e6a7-426c-a9ba-b0327186a803Original.jpg (pristupljeno: kolovoz 2019.)

[74] URL:https://www.gsmarena.com/apple_iphone_4s-4212.php (pristupljeno: kolovoz 2019.)

[75] URL: https://drop.ndtv.com/TECH/product_database/images/530201374038PM_635_iPhone_4.png (pristupljeno: kolovoz 2019.)

Popis kratica

ADB	(Android Debug Bridge) alat naredbenog retka koji omogućuje komunikaciju s uređajem
APK	(Android Package Kit) datoteke koje se koriste za prijenos i instalaciju mobilnih Android aplikacija
ASCII	(American Standard Code for Information Interchange) američki standard za razmjenu informacija
CC	(Carbon Copy) primatelji e-pošte
CD	(Compact Disc) medij za pohranu
CDMA	(Code Division Multiple Access) kodna raspodjela kanala
CMOS	(Complementary Metal Oxide Semiconductor) tehnologija izrade analognih i digitalnih mikroelektroničnih sklopova
CRC	(Cyclic Redundancy Check) način otkrivanja pogrešaka
DVD	(Digital Versatile Disc) optički disk koji se koristi za visokokvalitetno pohranjivanje informacija
EEP	(Evidence Export Process) izvozni proces digitalnih dokaza
EIP	(Evidence Import Process) uvozni proces digitalnih dokaza
eMMC	(Embedded MultiMedia Controller) memorija velike gustoće koja se nalazi u mobilnim uređajima
ESN	(Electronic Serial Number) identifikacijski broj kojeg proizvođači ugrađuju u mikročip mobilnih uređaja
GPS	(Global Positioning System) američki navigacijski satelitski sustav
GSM	(Global System for Mobile Communications) najrašireniji svjetski standard za mobilne komunikacije
ID	(Identity Document) identifikacijska oznaka određenog dokumenta
iDEN	(Integrated Digital Enhanced Network) mobilna telekomunikacijska tehnologija koja se zasniva na kompresiji govora i višestrukom pristupu i višestrukoj vremenskoj podjeli
IMEI	(International Mobile Equipment Identity) međunarodni broj mobilne opreme

iOS	(iPhone Operating System) operativni sustav Apple uređaja
IP	(Internet Protocol) mrežni protokol za prijenos podataka
ISO	(Internation Organization for Standardization) svjetska organizacija za standardizaciju
ISP	(In-System Programming) metoda je usmjerena uređajima koji sadrže eMMC *flash* čipove odnosno module.
JTAG	(Joint Test Action Group) udruga elektroničkih industrija za razvijanje metode provjere dizajna i ispitivanja tiskanih pločica nakon izrade
MAC	(Media Access Control) podsloj sloja podatkovne veze koji je odgovoran za prijenos paketa na i s kartice mrežnog sučelja
MDN	(Mobile Directory Number) desetoznamenkasti broj koji se bira za postizanje CDMA ili TDMA mobilnog uređaja
MIAT	(Mobile Internal Acquisition Tool) mobilni unutarnji alat za akviziciju
MIN	(Mobile Identification Number) desetoznamenkasti broj koji bežični operator koristi za identifikaciju mobilnog uređaja
MMS	(Multimedia Messaging Service) usluga slanja poruka koja uključuje multimedijske sadržaje
MTP	(Media Transfer Protocol) metoda ekstrakcije alata SPF Pro koja je usmjerena medijskim sadržajima
NFC	(Near Field Communication) bežična tehnologija za razmjenu podataka
PDA	(Personal Digital Assistant) mobilni terminalni uređaj koji je usmjeren pomaganju ljudima
PIM	(Personal Information Management) aktivnosti koje ljudi obavljaju u svrhu stjecanja, organiziranja, dohvaćanja i korištenja predmeta osobnih podataka
PIN	(Personal Identification Number) četveroznamenkasti kod koji se koristi za pristup SIM kartici
Plist	(Property List) datoteke svojstava koju koriste macOS aplikacije
RAM	(Random Access Memory) memorija s nasumičnim pristupom
RJ-45	(Registered Jack 45) kabel koji se koristi u strukturnom kabliranju
ROM	(Read Only Memory) memorija iz koje se podaci mogu samo čitati

SD	(Secure Digital) sigurna memorijska kartica
SIM	(Subscriber Identity Module) modul za identifikaciju pretplatnika
SOC	(System on a Chip) integrirani krug koji integrira sve komponente mobilnog uređaja
SPF Pro	(SmartPhone Forensic Professional) softverski forenzički alat tvrtke SalvationDATA
SQL	(Structured Query Language) standardni jezik za pohranu, manipuliranje i dohvaćanje podataka u bazama podataka
TAP	(Test Access Point) priključna točka na čipu
TDMA	(Time Division Multiple Access) vremenska raspodjela kanala
UFED	(Universal Forensic Extraction Device) najbolji alat mobilne forenzike
URL	(Uniform Resource Locator) putanja do određenog sadržaja na Internetu
USB	(Universal Serial Bus) tehnološko rješenje za komunikaciju računala s vanjskim uređajima
VPN	(Virtual Private Network) sigurna mreža koja koristi kriptiranu komunikaciju
XML	(Extensible Markup Language) jezik za označavanje podataka

Popis slika

Popis tablica