Forenzička analiza aplikacija za trenutačnu razmjenu poruka

Penava, Josip

Master's thesis / Diplomski rad

2024

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:119:251070

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-02-07**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Josip Penava

FORENZIČKA ANALIZA APLIKACIJA ZA TRENUTAČNU RAZMJENU PORUKA

DIPLOMSKI RAD

Zagreb, rujan 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Josip Penava

FORENZIČKA ANALIZA APLIKACIJA ZA TRENUTAČNU RAZMJENU PORUKA

FORENSIC ANALYSIS OF INSTANT MESSAGING APPLICATIONS

DIPLOMSKI RAD

Mentor: prof. dr. sc. Dragan Peraković

Student: Josip Penava

JMBAG: 0135240367

Zagreb, rujan 2024.

SAŽETAK

Ovaj diplomski rad opisuje metode i značajke forenzičke analize aplikacija za trenutačnu razmjenu poruka na Android operativnom sustavu. Sve većim korištenjem pametnih mobilnih telefona povećava se količina generiranih podataka od strane korisnika koji svakodnevno međusobnom interakcijom stvaraju digitalne dokaze čiji sadržaj može biti prikupljen i analiziran u istraživačke, edukacijske i pravne svrhe. U ovom diplomskom radu izvršena je ekstrakcija podataka Samsung pametnog mobilnog telefona prilikom koje je korišten softverski alat tvrtke Hancom. U radu su detaljno opisani postupci prikupljanja i analize podataka te su opisani dijelovi pojedinih podatak kao i mogućnosti koje sami alat može ponuditi istražitelju kako bi se izvršilo što vjerodostojnije i cjelovitije forenzičke analize. Posebno su opisane i zakonske legislative koje istražitelja ograničavaju i stavljaju u zadane okvire kako bi sami postupak forenzičke analize bio u skladu sa zakonom. Tijekom postupka forenzičke analize korišten je privatni uređaj autora ovog diplomskog rada kao i svi njegovi privatni podaci.

Ključne riječi: pametni mobilni telefon, aplikacija za trenutačnu razmjenu poruka, digitalna forenzička analiza, ekstrakcija podataka, analiza podataka, forenzički alati

SUMMARY

This master thesis describes the methods and features of forensic analysis of instant messaging applications on the Android operating system. The increasing use of smart mobile phones increases the amount of data generated by users who, through daily interaction, create digital evidence whose content can be collected and analyzed for research, educational and legal purposes. In this master thesis, the data extraction of the Samsung smartphone was carried out, during which the software tool of the company Hancom was used. The paper describes in detail the procedures for data collection and analysis, and describes parts of individual data as well as the possibilities that the tool itself can offer the investigator in order to perform the most credible and complete forensic analysis. The legal legislation that limits the investigator and places it within the given framework is also described in particular, so that the forensic analysis procedure itself is in accordance with the law. During the forensic analysis process, the private device of the author of this thesis was used, as well as all his private data.

Keywords: smart mobile phone, instant messaging application, digital forensic analysis, data extraction, data analysis, forensic tools

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 26. ožujka 2024.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Forenzička analiza informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 7509

Pristupnik: **Josip Penava (0135240367)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Forenzička analiza aplikacija za trenutačnu razmjenu poruka**

Opis zadatka:

U radu je potrebno prikazati aspekte korištenja pametnih telefona i aplikacije za trenutačnu razmjenu poruka. Opisati mogućnosti prikupljanja podataka aplikacija za trenutačnu razmjenu poruka. Opisati hardverske i softverske alate mobilne forenzike. Prikazati ekstrakciju podataka aplikacija za trenutačnu razmjenu poruk te mogućnosti analize ekstrahiranih podataka mobilnih aplikacija.

Mentor:

prof. dr. sc. Dragan Peraković

Predsjednik povjerenstva za diplomski ispit:

SADRŽAJ

1. Uvod 1
2. Korištenje pametnih telefona i aplikacije za trenutačnu razmjenu poruka 3
3. Prikupljanje podataka aplikacija za trenutačnu razmjenu poruka 8
   3.1 Uvod u aplikacije za trenutačno slanje poruka 8
      3.1.1 Memorijski sustavi Android uređaja 10
      3.1.2 Samsung Knox sigurnosni protokol 10
   3.2 Aplikacija Facebook Messenger 12
   3.3 Aplikacija WhatsApp Messenger 14
4. Hardverski i softverski alat mobilne forenzike 22
   4.1 Softver za forenzičku analizu 22
      4.1.1 MD – LIVE 22
      4.1.2 MD – NEXT 24
      4.1.3 MD – RED 25
   4.2 Hardver za forenzičku analizu 26
      4.2.1 MD – BOX 26
      4.2.2 MD - MR 27
      4.2.3 MD – READER 28
5. Ekstrakcija podataka aplikacija za trenutačnu razmjenu poruka 29
   5.1 Metode ekstrakcije 31
   5.2 Zakonska regulativa 33
   5.3 Ekstrakcija podataka s uređaja Samsung Galaxy S9 36
      5.3.1 Identifikacija pametnog telefona 37
      5.3.2 Postupak logičke ekstrakcije podataka 38
      5.3.3 Postupak fizičke ekstrakcije podataka 43
6. Analiza ekstrahiranih podataka mobilnih aplikacija 46
   6.1 Analiza podataka dobivenih logičkom ekstrakcijom 46
      6.1.1 WhatsApp 47
      6.1.2 Facebook Messenger 48
   6.2 Analiza podataka dobivenih fizičkom ekstrakcijom 49
      6.2.1 WhatsApp 49
      6.2.2 Facebook Messenger 53

6.3 Usporedba količine dobiveni podataka logičkom i fizičkom ekstrakcijom 54
7. Zaključak 56
LITERATURA 57
Popis kratica 60
Popis slika 62
Popis tablica 63
Popis grafikona 63

1. Uvod

Današnja svakodnevnica podrazumijeva korištenje pametnih mobilnih telefona kao glavnog asistenta prilikom rješavanja bilo kakvih dnevnih aktivnosti i zadaća koje za korisnika predstavljaju jednostavne ili zahtjevne radnje. Korištenje pametnih mobilnih telefona ne odnosi se samo na mlađu populaciju, što je do prije nekoliko godina bio slučaj, sada se sve više starije populacije želi i mora koristiti pametnim mobilnim telefonima kako bi ostali u korak s vremenom i mogli biti aktivni i ravnopravni dionici svakodnevnog života obavljajući općenite i složenije zadaće i poslove. Razumljivo je kako mlađi korisnici prednjače u količini sati provedenih koristeći pametne mobilne telefone koji za njih u nekim slučajevima predstavljaju *virtualnog prijatelja*, samim time kao posljedica toga je generiranje velike količine podataka koji se detaljnom analizom mogu koristiti kao kvalitetan uzorak definiranja korisnikovog ponašanja i predviđanja budućih aktivnosti.

Kako bi se generirane podatke uspješno analiziralo potrebno je provesti proces forenzičke analize kako bi ti podaci bili vjerodostojni i cjeloviti. Forenzička analiza je grana forenzičke znanosti koja se bavi ekstrakcijom i analizom podataka pohranjenih na digitalnim ili analognim uređajima. Podaci koji se prikupe forenzičkom analizom mogu se koristiti u istraživačke, edukacijske ili pravne svrhe što daje na važnosti takvom procesu u kojemu se koriste određene metodologije i prati vremenski slijed događaja kako bi prikupljeni podaci imali odgovarajuću razinu integriteta i vjerodostojnosti, [1].

S obzirom da veliki dio korisnika pametnih mobilnih telefona koristi aplikacije za trenutačnu razmjenu poruka koje generiraju veliku količinu podataka, u ovom diplomskom radu opisani su postupci prikupljanja i analize podataka pomoću specifičnog forenzičkog alata prateći određenu metodologiju. Kroz sedam cjelina ovoga diplomskog rada opisani su postupci generiranja i prikupljanja podataka od strane korisnika, te metode i postupci prikupljanja i analize podataka od strane istražitelja:

1. Uvod
2. Korištenje pametnih telefona i aplikacije za trenutačnu razmjenu poruka
3. Prikupljanje podataka aplikacija za trenutačnu razmjenu poruka
4. Hardverski i softverski alati mobilne forenzike
5. Ekstrakcija podataka aplikacija za trenutačnu razmjenu poruka
6. Analiza ekstrahiranih podataka mobilnih aplikacija
7. Zaključak

U drugom poglavlju detaljno je opisano korisničko korištenje pametnih telefona i aplikacija za trenutačnu razmjenu poruka gdje su navedene prednosti i nedostaci korištenja općenito pametnih telefona. Kroz grafove je prikazan porast korisnika u vremenskom periodu od deset godina te su prikazane kategorije aplikacija i postotak korištenja određene kategorije kako bi se dobio uvid u korisničku aktivnost.

Treće poglavlje opisuje načine prikupljanja podataka aplikacija za trenutačnu razmjenu poruka gdje su opisane same aplikacije i njihova arhitektura. Osim arhitekture samih aplikacija, opisani su i memorijski sustavi Android uređaja koji prikupljaju i pohranjuju korisničke podatke vrijedne za postupak forenzičke analize. Dodatno, opisan je i sigurnosni sustav Samsung Knox koji implementira skup protokola čija je zadaća onemogućavanje upada od strane stranih i zlonamjernih sustava. Dodatno, opisane su aplikacije Facebook Messenger i WhatsApp Messenger koje su jeden od vodećih aplikacija za trenutačnu razmjenu poruka.

U poglavlju *Hardverski i softverski alati mobilne forenzike* detaljno su opisani forenzički alati putem kojih se prikupljaju i analiziraju podaci važni za ovaj diplomski rad. Softverski alati potrebni za provedbu forenzičke analize tvrtke Hancom forenzičkom istražitelju omogućuju prikupljanje podatka i detaljnu analizu istih s preciznim grafičkim prikazom vremenskog slijeda događaja te filtraciju po vrsti podataka, vremenu i datumu nastajanja ili izmjene određenog podatka što je ključno za provedbu vjerodostojne forenzičke analize.

Peto poglavlje detaljno opisuje postupke i metode ekstrakcije podataka te se nadovezuje na zakonske regulative koje ograničavaju istražitelja u samom postupku ekstrakcije i analize. Nadalje, detaljno je opisan postupak identifikacije pametnog mobilnog telefona, postupak logičke ekstrakcije podataka i postupak fizičke ekstrakcije podataka čime je obuhvaćeno sve ono osnovno što spada u postupak forenzičke analize.

U zadnjem poglavlju objašnjena je analiza podataka dobivenih logičkom i fizičkom ekstrakcijom podataka koji su generirani od strane aplikacija za trenutačnu razmjenu poruka. Navedeni su podaci koje je generirao sam korisnik u interakciji sa svojim kontaktima i povezanim profilima u određenom vremenskom periodu.

2. Korištenje pametnih telefona i aplikacije za trenutačnu razmjenu poruka

Početak stoljeća obilježen je pokretom razvoja mobilne tehnologije koja može biti dostupna korisnicima bez obzira na njihovu lokaciju uz mogućnost nesmetanog korištenja mobilnih usluga poput telefonskih razgovora, slanja i primanja tekstualnih poruka, korištenja budilice, kreiranje kalendarskih oznaka, itd. Pojavom prvog iPhone-a 2007. godine započela je era razvoja pametnih mobilnih telefona koji su tada uz trenutne aktualne usluge imali mogućnosti poput slanja i primanja elektroničke pošte, pretraživanja weba, pretrage podataka i datoteka u samom uređaju i korištenje digitalne geografske karte, a sve to putem ekrana osjetljivog na dodir.

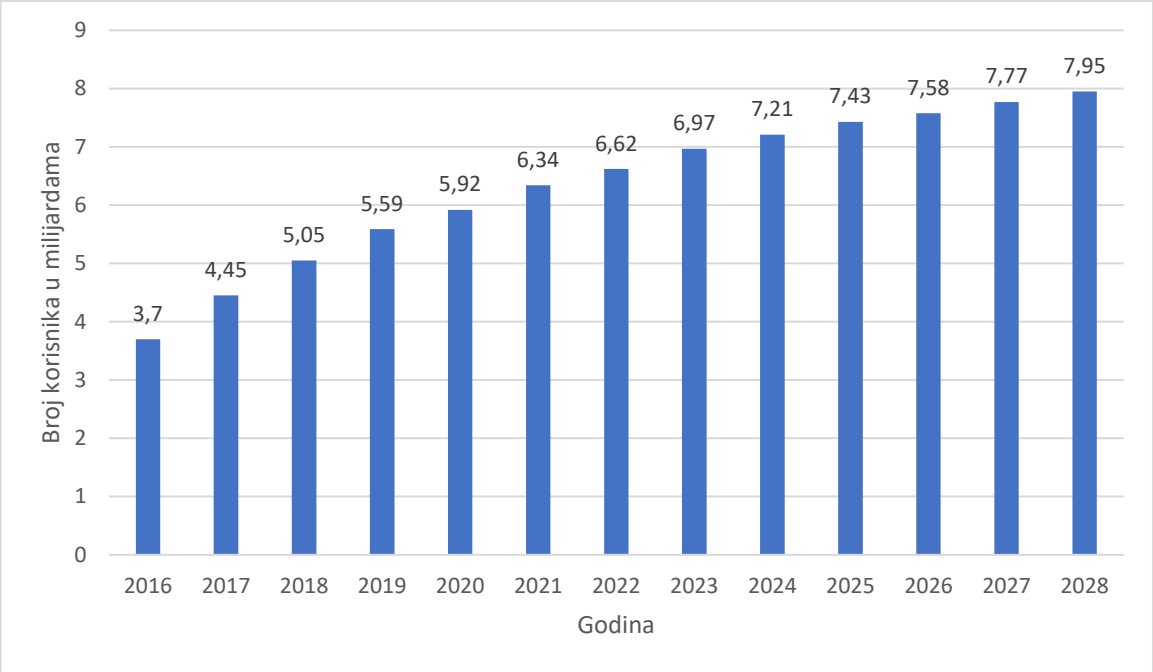
Nakon što su u pametne telefone integrirane kamere visoke rezolucije, mobilni telefoni postali su uređaji koji se koriste poput profesionalnih fotoaparata uz mogućnosti trenutnog dijeljenja sadržaja. Jednostavno rečeno pametni mobilni telefoni objedinili su nekoliko uređaja u jedan što je rezultiralo generiranjem velike količine podataka koji su pohranjeni u uređaju ili poslani putem informacijsko komunikacijske mreže. Kao što i računala pohranjuju svaku korisničku aktivnost tako to isto vrijedi i za pametne telefone koji sve više generiraju takvu vrstu podataka pomoću kojih se može odrediti, klasificirati i predvidjeti korisnikovo ponašanje i korisnikove želje.

Nezaobilazno je spomenuti istraživanje iz 2022. godine u kojemu se navode podaci da je u 2020. godini aplikacija za trenutačnu razmjenu poruka WhatsApp imala 2 milijarde korisnika, Facebook Messenger 1,3 milijarde korisnika a aplikacija WeChat 1,2 milijarde korisnika. Iz ovih podataka vidljivo je kako su aplikacije za trenutačnu razmjenu poruka dio svakodnevnice velike većine korisnika pametnih telefona, [2].

Zbog sve veće tendencije korištenja pametnih telefona u svakodnevnom životu, primijećeno je kako zaposlenici često koriste pametne telefone na radnom mjestu tijekom radnog vremena što može biti produktivno ali i kontraproduktivno, naravno što ovisi o poslodavcu i njegovom pristupu i razini implementacije pametnih telefona i uređaja u korporativno i poslovno okruženje.

Iz tog razloga sve više korisnika pomoću aplikacija za trenutačnu razmjenu poruka (engl. *Instant Messaging*, u nastavku IM) učinkovitije provodi zadatke vezane za posao ili privatne obaveze. U konceptu poslovne komunikacije IM je pokazao odlične rezultate iz razloga što korisnicima, tj. zaposlenicima, omogućava brzi odgovor na zahtjeve kupaca, brzi prijenos bitnih podataka a sve to uz zadovoljavajuću razinu sigurnosti kroz sučelje koje je jednostavno i dobro poznato krajnjim korisnicima, [3].

Kako bi se dobio uvid u količinu korištenja pametnih telefona na grafu 1 prikazan je broj pametnih telefona koji se na globalnoj razini koriste od 2016. godine do 2023. godine te procjena koliki broj uređaja će se koristiti do 2028. godine.

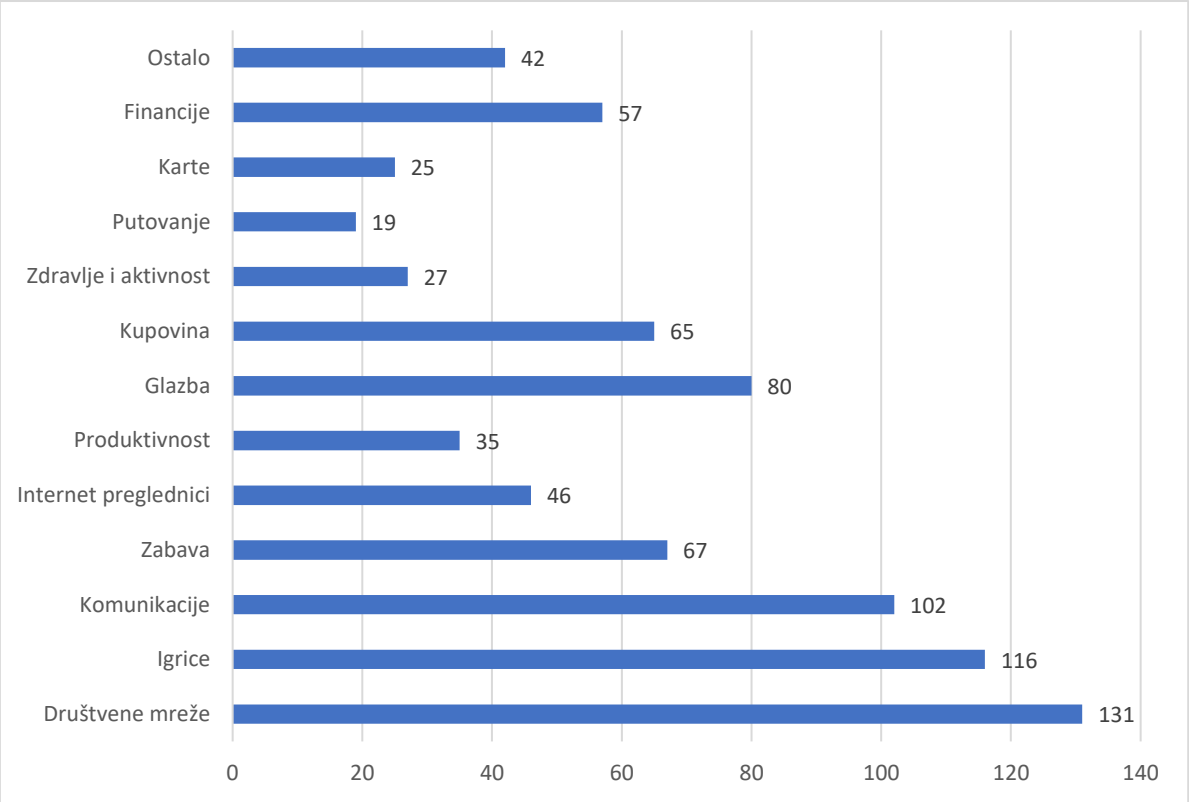


Grafikon 1. Broj korisnika pametnih telefona na globalnoj razini od 2012. do 2023. godine, [4]

Analizirajući prethodno prikazani graf, moguće je zaključiti kako broj korisnika pametnih telefona postepeno raste, godišnje u prosjeku 292,5 miliona korisnika, što kao posljedicu ima povećani intenzitet korištenja mobilni aplikacija, a samim time i aplikacija za trenutačnu razmjenu poruka. Korisnici koji najviše vremena provode koristeći značajke i aplikacije pametnih telefona su u kategoriji od 18 do 24 godine, te mjesečno provode 112,6 sati koristeći pametni mobilni uređaj, [5].

Korisnici u kategoriji od 25 do 34 godina mjesečno u prosjeku koristeći pametni telefon provedu 102,4 sata dok u kategoriji od 35 do 44 godina to vrijeme iznosi 93,6 sati. Na grafu 2 prikazano je prosječno vrijeme u minutama koje korisnici tjedno provedu koristeći određene kategorije aplikacija i funkcionalnosti pametnih telefona. Prethodno navedeni podaci prikazuju korisnikove navike koje imaju tendenciju da se sve više implementiraju u svaki aspekt čovjekova uobičajenog dana i uobičajenih obaveza.

Pametni telefon nije više samo uređaj za zabavu ili potrebu, on je naprosto postao dio korisnikove svakodnevnice koji je u najmanju ruku nezaobilazan. Koliko je pametni telefon postao dio korisnikova života pokazuju podaci kako 91% korisnika koristi uređaj kod kuće, 83% ga koristi tijekom tuširanja, 73% za vrijeme objeda, 72% na poslu ili u korporativnom okruženju, 79% kada je u društvu obitelji ili prijatelja, 71% čekajući u redu, 63% kada ide u kupovinu, 78% za vrijeme gledanja TV-a, te 62% u slučaju komunikacije vezane za obavljanje poslovnih procesa, [5].



Grafikon 2. Prikaz prosječnog vremena provedenog koristeći određenu kategoriju aplikacije u jednom tjednu, [5]

Iz prošlog odlomka vidljivo je kako se većina korisničke aktivnosti svodi na određeni vid interakcije između dva ili više korisnika što podrazumijeva isti broj uređaja putem kojih se odvijaju komunikacijski protokoli koji omogućavaju slanje i primanje tekstualnih poruka, fotografija, video zapisa, kratkih video zapisa bez zvuka (*gif*), audio zapisa, dokumenata, lokacija, poveznica i kontakata. Aplikacije za trenutačno poručivane (u nastavku IM) pridobile su pažnju korisnika kada je omogućeno slanje i primanje multimedijskih datoteka poput fotografija i video zapisa čime je korisnik vjernije moga prikazati i opisati željeni događaj ili osjećaj. Nije nepoznato kako korisnici sve više privatne komunikacije vrše putem ovakve vrste aplikacija čime uzročno posljedično stvaraju kolektivnu ovisnost o korištenju istih.

Osim konvencionalnog korištenja IM aplikacija u svrhu razmjene poruka između kontakata pohranjenih u pametnom telefonu, IM ima primjenu u konceptu korporativnog intraneta putem kojeg zaposlenici tvrtke ili organizacije mogu međusobno komunicirati bez upotrebe električne pošte. IM koriste mrežni operatori kako bi njihovi tehničari i komercijalisti uspješnije i efikasnije komunicirali s klijentima putem „chat“ sobe koja se generira na web stranici operatora. Iz prethodno navedenih potreba korisnika, IM aplikacije mogu biti izvedene kao mobilne aplikacije ili kao web temeljene aplikacije tj. IM usluge pružane putem računala.

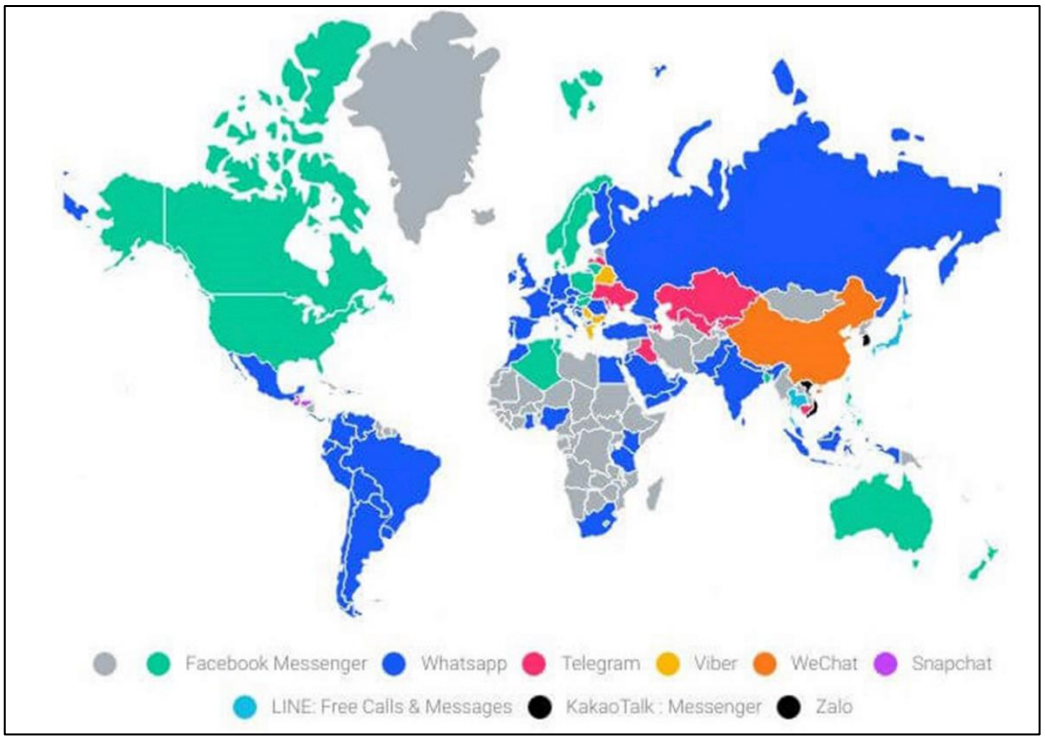
Povijest IM-a seže u 60-e godine prošlog stoljeća kada je nastala preteća ovakvoga sustava komuniciranja, što će biti opisano u nastavku. Glavne značajke aplikacija za trenutačno

poručivanje su primanje i slanje poruka te nadzor i informiranje o korisnikovoj aktivnosti. Praćenje korisnikove aktivnosti svodi se na prikupljanje podataka s centralnog servera o tome koji su trenutni kontakti (korisnici) aktivni i spremni primiti ili poslati poruku. U trenutku kontaktiranja željenog korisnika stvara se *chat* soba tj. strogo definirana konekcija koja korisnicima omogućava istovremenu komunikaciju, [6].

Jedna od najvećih kompanija u to vrijeme, AOL (engl. *America Online*), 1997. godine predstavila je inačicu IM-a pod nazivom *AOL Instant Messenger (AIM)* koja je korisnicima omogućavala informiranje o statusu drugih korisnika s *„buddy list“* popisa koji je sadržavao željene kontakte pojedinog korisnika. Krajem 80-ih i sredinom 90-ih godina prošlog stoljeća, za Internet korisnike koji nisu bili dio AOL sustava razvijeni su sustavi IRC (engl. *Internet Relay Chat*) i ICQ (engl. *I Seek You*) koji su omogućavali individualne i grupne razgovore, [7].

S krajem 1990-ih i s početkom 2000-ih godina dolazi od razvoja konkurentnih sustava poput *Yahoo!Messenger*-a koji je prilikom prijave zahtijevao Yahoo! ID, zatim je 1999. godine tvrtka *Microsoft* predstavila svoje IM rješenje pod nazivom MSN Messenger koji je direktno konkurirao AIM-u i Yahoo-u s 2,5 milijarde poslanih poruka dnevno. 2002. godine Apple pokreće iChat za korisnike Mac OS X operativnog sustava koji je kompatibilan s AIM-om, dok već 2003. godine započinje era video poziva predstavljanjem aplikacije *Skype* koja i dan danas ima pozamašan broj korisnika. Dvije godine kasnije Google predstavlja Google Talk koji postaje kompatibilan s Gmail sustavom čime korisnicima omogućava lakšu komunikaciju putem elektroničke pošte.

Kako bi ostao u utrci s konkurencijom Facebook 2008. godine predstavlja ekstenziju Facebook Chat koja je dio društvene mreže i ima veći potencijal za daljnji razvitak koji je potaknut promjenom imena 2014. godine u Facebook Messenger te predstavlja jednu od vodećih aplikacija za trenutačno slanje poruka. Pojavom WhatsApp-a 2009. godine korisnici integriraju s skupih SMS poruka na jednostavne i jeftine IM aplikacije čime je otvoreno novo tržište i natjecanje u prikupljanju željene publike. WhatsApp i Viber pioniri su u integraciji IM-a i VoIP-a (*engl.* Voice over IP) što kao rezultat daje veliku količinu prenesenih podataka koju generiraju korisnici svojom svakodnevnom aktivnošću.



Slika 1. Prikaz najkorištenijih IM aplikacija na uzorku od 100 zemalja, [8]

Na slici 1 prikazano je istraživanje korisničkog korištenja pojedine aplikacije za trenutačnu razmjenu poruka u 2022. godini na razini 100 zemalja od kojih je u njih 63 vodeća aplikacija WhatsApp dok je Facebook Messenger vodeći u 16 zemalja, Telegram u njih 10 dok je aplikacija Viber najkorištenija u Europi i to u zemljama poput Bjelorusije, Bugarske, Grče i Srbije.

3. Prikupljanje podataka aplikacija za trenutačnu razmjenu poruka

Iz podataka navedenih u prethodnom odlomku zaključivo je kako se većina korisnika pametnih telefona koristi aplikacijama za trenutačno slanje poruka što je nit vodilja ovoga diplomskog rada. Sve veća stopa konvencionalnog korištenja kao posljedicu daje eksponencijalan rast broja korisnika što je jedan od razloga za provedbu forenzičke analize nad ovom vrstom mobilnih aplikacija.

Da bi se forenzička analiza provela s uspjehom, tj. da rezultati budu transparenti i cjeloviti potrebno je objasniti strukturu IM aplikacija i njihove temeljne protokole koji osiguravaju sigurnu razmjenu poruka, poziva i multimedijskog sadržaja između korisnika. U ovom poglavlju opisati će se dijelovi arhitekture IM-a kao i XMPP protokol i ostale komponente zaslužne za sigurnu i cjelovitu komunikaciju.

Koncept *Instant Messaging* uz mobilne aplikacije koristi web temeljene aplikacije koje mogu biti kompatibilne s mobilnim aplikacijama, tj. dva ili više korisnika ne moraju biti na istovrsnim uređajima kako bi uspješno vršili komunikaciju. Iz tih razloga forenzičkoj analizi IM aplikacija dodaje se veća važnost pošto samim time obuhvaća veći broj korisnika, [9].

U nastavku opisati će se osnovni koncept IM-a koji je baziran na programskim rješenjima za stolna računala, nakon toga obratiti će se pozornost na XMPP protokol te naposlijetku na ono najbitnije, korištenje IM aplikacija na pametnim telefonima.

3.1 Uvod u aplikacije za trenutačno slanje poruka

Kako bi IM aplikacija imala svrhu potrebna su minimalno dva korisnika i jedan server koji će kontrolirati njihove statuse i prenositi poruke. U početnim fazama razvoja arhitektura IM-a bila je dosta jednostavna što u današnje vrijeme nije slučaj. Najjednostavniji opis takve arhitekture sačinjava softver instaliran na korisnikovo računalo koji korisniku omogućava komunikaciju s IM poslužiteljem („server“). Korisnik unosom korisničkog imena i lozinke postaje IM klijent čime mu je omogućeno korištenje IM funkcionalnosti koje se izvode na IM serveru.

Nakon što korisnik unese pripadajuće korisničko ime i lozinku smatra ga se prijavljenim („ulogiranim“), nakon čega korisnikovo računalo (IM klijent) šalje podatke poput IP adrese i broja porta IM poslužitelju kako bi uspješno ostvarili konekciju. IM poslužitelj kreira privremenu datoteku koja sadrži korisnikove podatke o konekciji te koja sadrži popis korisnikovih kontakata (drugi IM klijenti). IM poslužitelj provjerava koji korisnikovi kontakti su istovremeno prijavljeni na IM poslužitelj te korisnikovom IM klijentu šalje njihove konekcijske podatke, istovremeno IM poslužitelj šalje korisnikove podatke svim drugim korisnicima s korisnikove liste kontakata čime ih obavještava da je korisnik prijavljen i spreman za komunikaciju. Podaci o konekcijama IM klijentima omogućavaju slanje poruka izravno između sebe ili neizravno posredstvom IM servera. Ovakav koncept bio je prisutan u početcima IM-a

kada nije bilo davatelja internetskih usluga (ISP – „Internet Service Provider“). ISP [1]je omogućio korisniku korištenje IM usluga putem Interneta na način da je dopremao podatke o konekciji odgovarajućem IM poslužitelju. Osim toga ISP je zadužen za slanje poruka i ostalih datoteka između korisnika u istoj sesiji[2], [10].

Osim IM klijenta i IM poslužitelja, aplikacije za trenutnu razmjenu poruka koriste i IM multipleksore čija je uloga povećanje skalabilnosti, tj. upravljanje konekcijama. IM multipleksor ima zadaću sjedinjenja većeg broja konekcija u jednu TCP konekciju koja je povezana s IM poslužiteljem, tj. multipleksor čita podatke od pojedinih korisnika i zapisuje ih na IM poslužitelj, te obrnuto, čita podatke od IM poslužitelja i zapisuje ih na određenu točnu konekciju koja poruku prenosi IM klijentu koji ju tada prezentira korisniku kroz određeno aplikacijsko sučelje.

Kako bi se poruke multimedijalnog sadržaja od jednog korisnika prenijele drugom korisniku, koristi se direktna komunikacija između korisnika, bez posredstva IM servera, čime se ostvaruje znatno manje prometa (bitova) koji mogu biti preneseni u zadovoljavajućem vremenskom intervalu.

IM koncept temeljen je na dvije standardne arhitekture koje su okosnica ovakve vrste usluga. Prva arhitektura je klijentsko – poslužiteljska koja je korištena u većini slučajeva tj. koju koristi veći broj trenutno popularnih IM aplikacija. Glavna karakteristika ove arhitekture je ta da se poruke od korisnika A do korisnika B šalju posredstvom poslužitelja. Iz razloga što se povećava broj korisnika i njihova dnevna aktivnost, dolazi do potrebe za implementacijom većeg broja poslužitelja. Klijentsko – poslužiteljska arhitektura može biti izvedena na način da se implementira veći broj poslužitelja koji su pod nadzorom istog IM davatelja usluge ili to mogu biti grupe poslužitelja koje su pod nadzorom različitih davatelja IM usluga. Klijentsko – poslužiteljska arhitektura ima dvije izvedbe, simetričnu arhitekturu i asimetričnu arhitekturu. Simetričnu arhitekturu karakteriziraju grupe poslužitelja koji imaju identične funkcije, iz tog razloga klijent ne mora razlikovati poslužitelje i brinuti s kojim će komunicirati kako bi ostvario određene zahtjeve. Kod asimetričnog pristupa, svaki poslužitelj je zadužen za izvođenje određenih aktivnosti, bilo to prijava korisnika, otkrivanja drugih korisnika na mreži, provođenje cikličnih sigurnosnih kopija ili prosljeđivanje poruka. Inženjeri koji kreiraju aplikaciju za trenutačno prosljeđivanje poruka moraju odabrati određenu izvedbu s obzirom na razinu skalabilnosti koju žele implementirati u IM sustav tj. aplikaciju, [11].

Druga arhitektura je *peer-to-peer* ili korisnik-korisnik arhitektura koja ne sadrži poslužiteljske kapacitete. Ova vrsta arhitekture karakteristična je za prijenos multimedijskog sadržaja iz razloga što se podaci šalju direktno između dva korisnika bez posredstva poslužitelja što uvelike smanjuje kašnjenje te doprinosi skalabilnosti sustava.

[1] **Davatelj internetskih usluga** (engl. *Internet Service Provider,* akronim ISP), tvrtka koja korisnicima nudi usluge vezane uz pristup internetu i udomljavanje internetskih sadržaja (engl. *hosting*), tj. registriranje domene, smještaj mrežnih stranica, elektroničke pošte, mrežne trgovine i sl.

[2] Sesija je skup korisničkih interakcija s web-lokacijom koje se odvijaju unutar zadanog vremenskog okvira.

3.1.1 Memorijski sustavi Android uređaja

Forenzička analiza digitalnih uređaja temelji se na prikupljanju podataka iz memorije uređaja u kojoj mogu biti pohranjeni vrijedni podaci koji predstavljaju temeljne dokaze u istrazi. Alati za provedbu forenzičke analize su koncipirani i izvedeni na način da čitaju zapise u memorijskim pohranama terminalnog uređaja te ih prikazuju na način koji je razumljiv osobi koja provodi proces forenzičke analize. Iz tih razloga nezaobilazno je napomenuti neke dijelove pametnih mobilnih telefona koji su u fokusu istrage koja je provedena i opisana kroz ovaj diplomski rad.

Uz razne senzore, kamere, zaslone, procesore i jedinice napajanja, važnu ulogu u provedbi osnovnih zadaća pametnih telefona ima i memorijski kapacitet koji tvori funkcionalnu jedinicu unutar koje su pohranjeni podaci, instrukcije i programi koji omogućavaju nesmetan rad pametnog telefona. Podaci se u memoriju pohranjuju u binarnom obliku čime je memorijski kapacitet ograničen na maksimalni mogući broj upisanih nula i jedinica. Osnovna zadaća memorijskog sustava je pohrana i dohvaćanje podataka što je jedan od najvećih izazova za inženjere čiji je zadatak osigurati dovoljnu brzinu zapisivanja i čitanja podataka kako bi procesor nesmetano izvodio zadane instrukcije, [12].

Osnovna podjela memorijskih kapaciteta kod pametnih mobilnih uređaja je na radnu memoriju kojoj je potreban izvor napajanja kako bi sačuvala pohranjene podatke i trajna memorija kojoj nije potrebno napajanje za očuvanje podataka tj. koja je trajna. Trajna ili *flash* memorija najčešće dolazi u dvije izvedbe, to su NOR i NAND. NOR memoriju karakterizira brzi odziv i provođenje procesa čitanja podataka, dok je zapisivanje podataka sporije nego kod NAND memorije. NAND memorija omogućava veći kapacitet pohrane podataka uz napomenu da je NAND memorija manje stabilna od NOR memorije. RAM memorija spada pod kategoriju radne memorije koja pohranjuje podatke bitne za trenutne aktivnosti i programe koji se izvode na uređaju. Sadržaj RAM memorije karakteriziraju podaci vezani za izvođenje aplikacija koje procesor uređaja može dohvatiti i do 10 puta brže nego podatke koji su pohranjeni na vanjskim memorijskim kapacitetima poput eksterne SD kartice, [13].

3.1.2 Samsung Knox sigurnosni protokol

Kako bi Samsung omogućio svojim korisnicima bezbrižno i sigurno korištenje pametnih terminalnih uređaja, implementirao je skup protokola pod imenom *Root of Trust* što bi u prijevodu značilo „korijen povjerenja“, a misli se na proces pokretanja operacijskog sustava uređaja po određenim protokolarnim koracima koji omogućavaju veću razinu zaštite osnovnih pokretačkih programa. Implementacijom takvog protokola smanjuje se stupanj izloženosti sustava, a samim time i podataka pohranjenih na uređaju, omogućava se otkrivanje neželjenih upada u sustav od strane drugih sustava, uz to *Root of Trust* implementira mehanizam za zaključavanje osjetljivih podataka. Glavna odlika ovog sigurnosnog protokola je ta da niz

strogih provjera počinje već na hardverskoj razini i nastavlja se na softversku razinu, a pošto je hardverom teže manipulirati smatra se da je sustav samim time zaštićeniji.

U nastavku su navedeni koraci koji opisuju implementaciju i rad *Root of Trust* protokola na Samsung uređajima:

1. Knox sigurnosna platforma počinje s implementacijom već u procesu proizvodnje pametnog telefona kada se uz pomoć *Device-Unique Hardware Key*-a (*DUHK*) generira nasumični brojevni zapis,
2. Zatim DUHK generira i kriptira *Device Root Key (DRK)* i *Samsung Attestation Key (SAK),*
3. Kada je uređaj pokrenut, Samsung uz pomoć *Samsung Secure Boot Key*-a (*SSBK*) provjerava sve softverske komponente. *TrustZone Secure* okruženje pohranjuje sigurnosne kodove koji su čitljivi samo specijalnim softverskim modulima koji uz pomoć *TrustZone Secure* okruženja mogu čitati sigurnosne kodove.
4. Prije pokretanja, softver provjerava svaku značajku Knox platforme čime je omogućena detekcija napada na bilo koji dio lančane provjere koja se izvršava od hardverskog pa sve do softverskog modula pokretanja uređaja.

Visoka razina zaštite implementirana je na prvom sloju Knox sigurnosnog protokola, a sastoji se od jednokratnih osigurača kao što su mehanizmi šifriranja ključeva, prevencije vraćanja stare verzije OS-a i Knox jamstva. U ovom slučaju opisati će se prevencija vraćanja stare verzije OS-a koja je nazvana *Rollback Prevention (RP)* osigurač. RP osigurač radi na principu kodiranja posljednje prihvatljive verzije Samsung *bootloader*-a. Iz razloga što u nekim starijim verzijama postoje poznate ranjivosti koje mogu iskoristiti zlonamjerni korisnici, RP onemogućava vraćanje starije verzije *bootloader*-a. RP prilikom instalacije softvera i ažuriranja istog generira RP broj verzije osigurača koji nakon što je implementiran onemogućava vraćanje na stare verzije softvera, [18].

Ono što je još važno za dostatnu razinu zaštite pametnog telefona odnosi se na zaštitu kernela, tj. jezgre Android sustava zasnovanog na Linux OS-u. Kernel predstavlja poveznicu između hardvera i softvera što ga čini najnižim apstrakcijskim slojem operacijskog sustava. Knox je implementacijom *Real-time Kernel Protection (RKP)* zaštitnog mehanizma omogućio jaču zaštitu od zlonamjernih manipulativnih radnji koje bi mogle dovesti do gubitka podataka, ucjene, špijunskih aktivnosti ili nekih drugih neželjenih scenarija. RKP je dizajniran na način da se izvršava u izoliranom i pouzdanom okruženju, samim time smanjuje mogućnost modificiranja naredbi pohranjenih u kernelu čime uvelike smanjuje mogućnost zlonamjerne manipulacije i povećava vrijeme trajanja procesa neovlaštenog upada u inicijalne postavke uređaja. RKP zaštita grupirana je u tri zone:

- **Kernel kod** – RKP onemogućava izmjenu kodova i logičkih veza,
- **Kernel podaci** – RKP onemogućava izmjenu datotečnih struktura kritičnih za ispravan rad kernela,
- **Kernel kontrola toka** – RKP onemogućava reverzibilno programiranje koje može biti korišteno u procesu napada na uređaj

Osim prethodno navedenog, Knox je implementirao značajku pod nazivom *Periodic Kernel Measurement (PKM)* čija je zadaća periodično nadziranje kernela kako bi se detektirale i spriječile neželjene promjene u izvornom kodu. Kako bi PKM znao koji kodovi su izvorni koristi se SHA1 *hash* enkripcija za potvrdu autentičnosti i cjelovitosti zapisa, [14].

3.2 Aplikacija Facebook Messenger

Jedna od 10 najkorištenijih aplikacija za trenutačnu razmjenu poruka je Facebook Messenger (u nastavku FM) koji je u vlasništvu mega kompanije Facebook. Kompanija Facebook osnovana je 2004. godine u Sjedinjenim Američkim Državama od strane nekoliko osnivača, Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz i Chris Hughes. Facebook je u početcima za razmjenu poruka između korisnika koristio Facebook Chat aplikaciju koju je 2011. godine zamijenila Facebook Messenger aplikacija. FM je aplikacija koja ne zahtijeva kreiranje korisničkog računa na glavnoj platformi Facebook-u, čime omogućava korištenje usluga slanja i primanja korisnicima koji ne žele ili nemaju aktivan Facebook račun, tj. profil. FM aplikacija dostupna je na Android i iOS operacijskim sustavima čime privlači veliki broj korisnika a samim time i generiranih poruka, to dokazuje podatak da je u 2020. godini u prosjeku dnevno generirano 8 milijardi poruka od strane FM korisnika.

Kao i sve IM aplikacije i Facebook Messenger korisnicima omogućava slanje tekstualnih poruka u individualnim ili grupnim razgovorima, uz to omogućava slanje fotografija, video zapisa, audio zapisa, naljepnica i GIF-ova. Neke od značajki su i opcije prikazivanja kada drugi korisnik tipka poruku, isto kao i status o poruci tj. je li poruka isporučena, zaprimljena te točno vrijeme primitka poruke. Prilikom slanja i primanja fotografija i video zapisa FM prikuplja generirane datoteke u jedinstvenu mapu gdje korisnik može manipulirati istim tim datotekama. Korisnik ovisno o želji može izbrisati, arhivirati ili ponovno prikazati poruke čime može onemogućiti prikazivanje određenog sadržaja, s time da najnovija verzija iz svibnja 2021. godine omogućava arhiviranje cjelokupnog razgovora.

Osim uobičajenih IM značajki, FM korisnicima omogućava pokretanje video i audio poziva prema ostalim korisnicima koji imaju pristup Internetu čime je omogućena besplatna konverzacija u stvarnom vremenu, kašnjenje ovisi samo o stabilnosti i brzini Internetske veze korisnika.

FM korisnicima u Sjedinjenim Američkim Državama koji su stariji od 18 godina nudi uslugu slanja novca putem FM aplikacije na način da se u privatnom razgovoru pod kategorijom *Meni* odabere opcija *Send Money,* naravno ukoliko su prethodno upisani i pohranjeni podaci o kreditnoj ili debitnoj kartici i bankovnom računu oba korisnika.

Neki od dodatnih mogućnosti su igranje video igara u aplikaciji neovisno o tome je li korisnik u privatnom ili grupnom razgovoru. Popularna značajka je dijeljenje lokacije koja drugim korisnicima omogućava praćenje lokacije korisnika koji ju dijeli u narednih sat vremena od trenutka dijeljenja lokacije.

Ukoliko korisnik pošalje poruku koja u sebi sadrži referencu na određeni datum, FM aplikacija automatski korisniku nudi opciju *Podsjetnici* čime omogućava stvaranje podsjetnika na neke bitne događaje. Važno je napomenuti kako FM ima opciju stvaranja nadimaka za individualne ili grupne razgovore, te omogućava promjenu teme za svaki pojedini razgovor. Ukoliko korisnik ne želi slati tekstualnu poruku, FM pruži mogućnost snimanja audio isječaka koji mogu sadržavati bitne informacije, uz napomenu da se prilikom snimanja audio isječka korisnik isto tako može koristiti tipkovnicom, [15], [16].

Facebook je kao jednu od metode razvoja svoje baze podataka emigrirao s HBase baze podataka na MyRocks bazu podataka koja im je ostvarila nekoliko važnih prednosti u odnosu na konkurenciju. Implementacijom MyRocks baze podataka povećala se je brzina, pouzdanost i skalabilnost same baze podataka što je korisnicima omogućilo brže i interaktivnije iskustvo korištenja aplikacije. Ovime je redizajnirana i pojednostavljena sama shema baze podataka što kao posljedicu ima brže i točnije formatiranje podataka, uz to da je kao novitet potrebno napomenuti kako MyRocks koristi Facebook-ov projekt otvorenog koda u kojemu je integrirana RockDB baza podataka izvodeći se na MySQL platformi, [17].

Iz razloga što se ovaj diplomski rad temelji na forenzičkoj analizi pametnog telefona i na njemu instaliranih aplikacija za trenutačnu razmjenu poruka, nezaobilazno je navesti neke komponente cjelokupne arhitekture baze podataka koja se pohranjuje na sami uređaj. Koristeći se navedenim izvorima podataka [16], u nastavu će se navesti neke od SQL tablica koje su prikupljene u forenzičkima analizama drugih istražitelja. U ovom slučaju istražitelj je koristeći forenzičke alate XRY i Oxygen prikupio i analizirao prikupljene datoteke sa uređaja Samsung Galaxy S5. Analizom je otkriveno da postoje šest tablica u bazi podataka, od kojih je detaljnije obrađena tablica *address_table*. U tablici 1 navedena su imena atributa i vrsta podatka za pojedini redak prethodno navedenih tablica.

Tablica 1. Popis podataka u tablici *address_table*

Tablica *address_table*	
Ime atributa	**Vrsta podatka**
address	TEXT
smsc	TEXT
delete_score	REAL
delete_score_ts	INTEGER
spam_score	REAL
ranking_score	REAL
cores_ts	INTEGER

Izvor: [18]

Prethodno opisani slučaj provedene forenzičke analize nad aplikacijom Facebook Messenger biti će temeljni orijentir prilikom provedbe forenzičke analize koja će biti izvedena pomoću softverskih forenzičkih alata MD – RED i MD – NEXT tvrtke HANCOM. Postupci provedeni tijekom istrage temelje se na NIST standardu koji će biti detaljno opisan u poglavlju *4. Hardverski i softverski forenzički alati*.

3.3 Aplikacija WhatsApp Messenger

Nezaobilazna aplikacija za trenutačnu razmjenu poruka WhatsApp Messenger (u nastavku WhatsApp) zasigurno je najkorištenija IM aplikacija na svijetu i samim time njeni korisnici generiraju najveću količinu podataka. WhatsApp svojom jednostavnošću i mogućnostima privlači sve veći broj korisnika što potvrđuje brojka od 2 milijarde korisnika u listopadu 2019. godine. Zbog ovolike zainteresiranost WhatsApp stoji uz rame renomiranim aplikacijama kao što su Facebook i YouTube koji sve intenzivnije kreiraju ponašanje i navike korisnika. Osnivači WhatsApp-a su Jan Koum i Brian Acton koji su 2009. godine potaknuti i vođeni iskustvom kojeg su stekli radom u Yahoo – u stvorili aplikaciju za pametne mobilne uređaje čija je glavna značajka bila zamjena za SMS poruke. Kreatori aplikacije korisnicima su omogućili registraciju na osnovu mobilnog pretplatničkog broja što uvelike pojednostavljuje sami proces registracije s naglaskom da nakon prve prijave u aplikaciju od korisnika se više ne zahtjeva prijava, sve do promjene mobilnog uređaja ili mobilnog pretplatničkog broja.

Naravno, kao i sve druge aplikacije za trenutačno prosljeđivanje poruka, WhatsApp sadrži razne mogućnosti razmjene multimedijskih datoteka, lokacija, dokumenata, kratkih audio poruka, te opcije iniciranja ili prihvaćanja video i audio poziva. Upravo video i audio pozivi su proslavili aplikaciju iz razloga što je korisnicima ukoliko imaju pristup Internetu omogućen razgovor s jednim ili više željenih korisnika bilo to video pozivom ili audio pozivom. Nestvarno je kako su mogućnosti i značajke pametnih telefona napredovale do te mjere da u današnje vrijeme korisnici mogu voditi razgovore u stvarnom vremenu, udaljeni tisućama kilometara i to sve uz minimalne novčane naknade (ovisno o tarifiranju od strane davatelja usluge i mogućnosti pristupu Wi-Fi mreži). Jan i Brian imali su viziju o aplikaciji koja bi što efikasnije i preciznije zamijenila svakodnevni razgovor što dokazuje činjenica da su objedinili frazu „*What is Up*“ što je između ostalog olakšalo marketinške aktivnosti. 2014. godine WhatsApp se pridružuje Facebook grupaciji čime započinje kampanja dijeljenja podataka s Facebook kompanijom. WhatsApp zbog poboljšanja performansi izvođenja aplikacije, povećanja sigurnosnih i integritetnih protokola te lakših analitičkih procesa od korisnika prikuplja i prosljeđuje određene vrste podataka. Podaci vezani za korisnikov uređaj odnose se na jedinstveni identifikator uređaja, broj verzije OS-a, broj verzije aplikacije, pretplatnički kod države i pretplatnički kod mreže, dok se podaci vezani za korištenje aplikacije odnose na vremensku oznaku zadnjeg korištenja aplikacije, datum prve registracije korisničkog računa te način i učestalost budućeg korištenja WhatsApp funkcionalnosti, [19].

WhatsApp osim što omogućuje individualne i grupne razgovore (predefiniran broj korisnika u grupi je 256) te korištenje aplikacije sinkrono na mobilno uređaju i stolnom tj. prijenosnom računalu, omogućava *end-to-end* enkripciju poruka i razgovora koja je opisana u nastavku.

Generalna značajka *end-to-end* enkripcije poruka je ta da poruka koju korisnik pošalje drugom korisniku nitko drugi osim te dvije strane ne može pročitati, tj. poruka je šifrirana određenom metodom te ju samo pošiljatelj i primatelj pomoću odgovarajućeg kriptografskog ključa mogu dekriptirati i pročitati bez da je sadržaj poruke izmijenjen, izbrisan ili pročitan od neke treće strane. Enkripcija se izvodi pomoću matematički strukturiranih kripto algoritama koji pretvaraju željene podatke (tekst, fotografija, dokument video i audio zapis) u nasumično

odabran tekst, tj. algoritamski odabran tekst koji nema nikakvo značenje za čovjeka. Takav nerazumljiv tekst šalje se putem Interneta do primatelja koji ga zaprima na svom uređaju u istom tom obliku, nakon čega se kriptografskim ključem tekst pretvara u oblik razumljiv čovjeku. WhatsApp u svojoj *end-to-end* metodi koristi dvije vrste kriptografskih ključeva tj. algoritama, asimetrični i simetrični. Simetrični ključevi osiguravaju povjerljivost i cjelovitost poslanih podataka, dok asimetrični algoritmi omogućavaju autentifikaciju i nepobitnost. Kod simetričnih ključeva implementiran je samo jedan ključ koji se koristi za šifriranje i dešifriranje podataka, dok se kod asimetričnih ključeva koriste dva zasebna ključa. Smisao asimetričnih ključeva je ta da se podaci koji su šifrirani pomoću javnog ključa od strane pošiljatelja mogu dešifrirati samo pomoću privatnog ključa tog istog pošiljatelja, što isto tako vrijedi i za primatelja, [19].

Aplikacija WhatsApp za šifriranje poruka koristi Signal Protocol tvrtke Open Whisper Systems. Signal Protocol implementira Double Ratchet algoritam, Triple Diffie Hellman (X3DH), AES, HMAC SHA256 i Curve25519 algoritam (Eliptic Curve Diffie Hellman algoritam). Curve25519 uveden je nakon što je NSA optužena da je zloupotrijebila P-256 NIST standard kako bi presretala podatke poslane putem Interneta. U nastavku je u četiri koraka pojašnjeno kako WhatsApp pomoću end-to-end kriptiranja prenosi poruke s velikom razinom povjerljivosti i cjelovitosti podataka:

1. Javni i privatni ključ generiraju se prilikom prve aktivacije aplikacije na korisnikovom pametnom telefonu.
2. Privatni ključ ostaje pohranjen na korisnikovom uređaju dok se javni ključ šalje posredstvom WhatsApp servera drugom korisniku tj. primatelju.
3. Javni ključ šifrira pošiljateljevu poruku na njegovom uređaju prije nego ona bude poslana na WhatsApp server.
4. Server se koristi samo za prosljeđivanje šifriranih poruka, dok samo primateljev privatni ključ može dešifrirati poruku. Ovime se postiže da niti jedna treća strana ne može vidjeti sadržaj poruke.

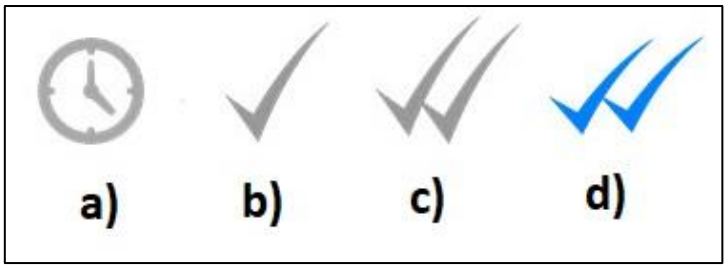
Kako bi korisnik ručno provjerio šifriranje između sebe i drugoga kontakta, pod opcijom *Šifrifanje* na kartici *Info* vezanoj za određeni kontakt moguće je vizualno pregledati 60-znamenkasti kod ili skeniranjem QR koda provjeriti jesu li podaci o šifriranju identični. Na slici 2 prikazan je jedan takav QR kod s popratnim 60-znamenkastim kodom, [20].

Neke od za forenzičku analizu zanimljivih značajki WhatsApp-a je opcija *Nestajuće poruke* što je već viđeno u aplikaciji Telegram. Ova opcija korisniku omogućava brisanje poruka iz određenog razgovora sedam dana nakon slanja ili primanja iste, druga strana (korisnik) ne mora imati uključenu ovu opciju te će se na njegovom uređaju poruke uspješno pohraniti.

Slika 2. Prikaz QR i 60-znamenkastog koda za provjeru enkripcije

Izvor: Autor (osobni primjer)

Jedna od glavnih i prepoznatljivih značajki WhatsApp aplikacije su indikatori u obliku jedne ili dvije kvačice koji korisnika obavještavaju o statusu poslane poruke. To znači da u slučaju kada pošiljatelj stisne gumb za slanje poruke, u desnom donjem uglu okvira poruke, se pojavljuje ikona koja nalikuje na sat (slika 3, oznaka a) i upućuje korisnika na to da je njegova poruka u procesu slanja, tj. šalje se na WhatsApp server. Kada se umjesto ikone sata pojavi ikona jedne kvačice (slika 3, oznaka b) WhatsApp signalizira da je poruka uspješno poslana na server i čeka da ju drugi korisnik (primatelj) preuzme. U trenutku pojave druge kvačice (slika 3, oznaka c), primatelj je zaprimio poruku ali ju nije pročitao, tj. nije ušao u razgovor kako bi signalizirao da je poruka pročitana. Kada primatelj uđe u razgovor smatra se da je poruka pročitana što WhatsApp signalizira pomoću dvije plave kvačice (slika 3, oznaka d).



Slika 3. Znakovi statusa poruke WhatsApp aplikacije

Izvor: Autor (osobni primjer)

Osim toga, korisnicima je omogućeno informiranje o trenutku posljednje aktivnosti drugog korisnika što je jedna od važnijih funkcionalnosti kada je riječ o forenzičkoj analizi pametnog telefona i aplikacija za trenutno poručivanje. Datum i vrijeme slanja i primanja poruke od velike je važnosti za bilo kakvu vrstu istrage iz razloga što se kreiranjem vremenske crte može lakše detektirati, analizirati i zaključiti određeni postupak od strane korisnika čiji je uređaj predmet istrage.

Kao i svaka mobilna aplikacija, tako i WhatsApp pohranjuje određene podatke na korisnikov uređaj, što može značiti da se određeni podaci poput kontakata i log zapisa pohranjuju na lokalnu memoriju uređaja dok se podaci kao što su fotografije i video zapisi pohranjuju na vanjsku memoriju uređaja (*microSD* kartica). U sljedećim odlomcima ovoga diplomskog rada okvirno su objašnjene dvije temeljne baze podataka koje su generirane od strane WhatsApp-a prilikom instalacije aplikacije, te čiji sadržaj generira korisnik tijekom korištenja iste. Datoteke koje se spominju u većini članaka i znanstvenih radova su *wa.db* i *msgstore.db* koje su kreirane u *SQLite* programskom alatu, a čija je struktura navedena u nastavku, [20], [21].

Na informativnoj stranici *Magnet Forensics* organizacije ukratko je opisana struktura prethodno spomenutih baza podataka koje se odnose na listu kontakata i poruka pohranjenih u WhatsApp aplikaciji.

Baza podataka *msgstore.db* sadrži 20-ak tablica od kojih će neke biti opisane u nastavku rada. Neke od bitnih informacija ove baze podataka su telefonski brojevi pohranjenih kontakata, sadržaj poruke, status poruke i vremenske oznake. Poruke koje sadrže privitke imaju vrijednost *NULL* što znači da nema sadržaja ali je naveden link ili ikona koja istražitelja upućuje na drugi dio baze podataka u kojemu su pohranjeni poslani i primljeni prilozi. Takve datoteke poput fotografija, audio ili video zapisa mogu sadržavati podatke poput zemljopisne širine i visine što omogućava lociranje geografske lokacije na kojoj je zapis stvoren. *Msgstore.db* koja je pohranjena u Android uređajima na datotečnoj putanji */data/data/com.whatsapp/databases/* sadrži sljedeće tablice: *chat_list, conversion_tuples, deleted_chat_jobs, frequents, group_participiants, group_participiants_history, labeled_jids, labeled_messages, labels, media_refs, media_streaming_sidecar, message_thumbnail, messages, messages_edits, messages_fts_content, messages_fts_segdir, messages_fts_segments, messages_links, messages_quotes, messages_vcards, messages_vcards_jids, props, receipts, sqlite_sequence* i *status_list.* Od ovih navedenih tablica

neke su više a neke manje zanimljive u kontekstu forenzičke analize, te će se iz tog razloga u nastavku opisati tablice koje sadrže bitne podatke za istragu:

- ***Sqlite_sequence*** - tablica koja sadrži općenite informacije o bazi podataka, instancama, ukupnom broju pohranjenih poruka, ukupnom broju razgovora i ostalo.
- ***Message_fts_content*** – tablica koja sadrži detalje razgovora poredanih po vremenu nastanka.
- ***Messages*** – tablica koja sadrži informacije o broju telefona kontakta, sadržaju poruke, statusu, vremenskim oznakama i podacima o privitcima. U tablici 2 navedena je struktura *messages* tablice u obliku imena stupca i značenja istog.

Tablica 2. Struktura *messages* tablice WhatsApp *msgstore.db* baze podataka

OZNAKA	ZNAČENJE
_id	Sekvencijalni broj zapisa (generira SQLite)
Key_remote_jid	WhatsApp ID sugovornika
Key_from_me	Vrsta poruke: '0'=dolazna, '1'=odlazna
Key_id	Jedinstveni identifikator poruke
Status	Status poruke: '0'=primljena, '4'=čeka na serveru, '5'=isporučena na odredište, '6'=kontrolna poruka, '13'=poruka otvorena od strane primatelja (pročitana)
Need_push	'2'=*broadcast* poruka, '0'=ostalo
Dana	Sadržaj poruke kada je *media_wa_type*='0'
Timestamp	Sadrži vremenske oznake u *Unix Epoch Time (ms)* formatu, vrijednost preuzeta s uređaja
Media_url	URL prenesene datoteke kada je *media_wa_type*='1', '2', '3'
Media_mime_type	MIME vrsta prenesene datoteke kada je *media_wa_type*='1', '2', '3'
Media_wa_type	Vrsta poruke: '0'= tekst, '1'= fotografija, '2'= audio zapis, '3'= video zapis, '4'= kontakt, '5'= lokacija
Media_size	Veličina prenesene datoteke kada je *media_wa_type*='1', '2', '3'
Media_caption	Sadrži riječi „audio“ i „video“ kada je *media_wa_type*='1', '3'
Media_hash	Base64-encoded SHA-256 hash vrijednost prenesene datoteke kada je *media_wa_type*='1', '2', '3'
Origin	'2'=*broadcast* poruka, '0'=ostalo
Latitude	Zemljopisna širina pošiljatelja kada je *media_wa_type*='5'
Longitude	Zemljopisna visina pošiljatelja kada je *media_wa_type*='5'
Thumb_image	Osobni podaci
Remote_recource	ID pošiljatelja (samo za grupne razgovore)
Received_timestamp	Vrijeme primanja poruke, vremenska oznaka u *Unix Epoch Time (ms)* formatu, vrijednost preuzeta s uređaja
Send_timestamp	Nekorišten, uvijek postavljen na '-1'

Receipt_server_timestamp	Vrijeme primanja ACK poruke od servera, vremenska oznaka u *Unix Epoch Time (ms)* formatu, vrijednost preuzeta s uređaja
Receipt_device_timestamp	Vrijeme primanja ACK poruke od primatelja, vremenska oznaka u *Unix Epoch Time (ms)* formatu, vrijednost preuzeta s uređaja
Read_device_timestamp	Vrijeme otvaranja (čitanja) poruke, vremenska oznaka u *Unix Epoch Time (ms)* formatu, vrijednost preuzeta s uređaja
Played_device_timestamp	Vrijeme reprodukcije poruke, vremenska oznaka u *Unix Epoch Time (ms)* formatu, vrijednost preuzeta s uređaja
Raw_data	Sličica prenesene datoteke kada je *media_wa_type*='1', '3'
Recipient_count	Broj primatelja (*broadcast* poruka)

Izvor: [20], [21]

- **Messages_thumbnails** – tablica sadrži informacije o prenesenim fotografijama
- **Chat_list** – tablica sadrži informacije o razgovorima koje detaljno opisuju koji korisnik je pošiljatelj a koji primatelj te u kojem trenutku su poruke poslane ili primljene

Baza podataka *wa.db* sadrži detaljne informacije o pojedinom kontaktu pohranjenom na korisnikovom uređaju kao što je detaljan prikaz broja telefona, imena ili nadimka za određeni kontakt te nekih napomena koje mogu biti korisne tijekom istrage. Prema izvoru [20] i [21] *wa.db* koja je pohranjena u Android uređajima na datotečnoj putanji */dana/dana/com.whatsapp/databases/* sadrži sljedeće tablice: *android_metadata, sqlite_sequence, system_contacts_version_table, wa_biz_profiles, wa_biz_profiles_websites, wa_contact_capabilities, wa_contact_storage_usage, wa_contacts, wa_group_descriptions, wa_vnames* i *wa_vnames_localized.* Naravno da je jedna od najzanimljivijih tablica za forenzičku analizu *wa_contacts* koja sadrži pojedinosti o kontaktima koji su uključeni u individualne ili grupne razgovore, a čija je struktura prikazana u tablici 3.

Tablica 3. Struktura *wa_contacts* tablice u WhatsApp *wa.db* bazi podataka

OZNAKA	ZNAČENJE
_id	Sekvencijalni broj zapisa (generira SQLite)
jid	ID oznaka kontakta od strane aplikacije (struktura: 'x@s.whatsapp.net', gdje 'x' označava broj telefona korisnika)
is_whatsapp_user	Sadrži '1' ukoliko je kontakt Whatsapp korisnik, inače '0'
status	Tekst koji opisuje status kontakta
status_timestamp	Sadrži vremensku oznaku u *Unix Epoch Time (ms)* formatu
number	Broj telefona povezan s kontaktom
raw_contact_id	Ime kontakta prikazano na zaslonu
phone_type	Vrsta pametnog mobilnog telefona
phone_label	Oznaka povezana s brojem telefona
unseen_msg_count	Broj poruka poslan određenom kontaktu koje su isporučene ali nisu pročitane.
Photo_ts	Sadrži vremensku oznaku u *Unix Epoch Time* formatu
thumb_ts	Sadrži vremensku oznaku u *Unix Epoch Time* formatu

photo_id_timestamp	Sadrži vremensku oznaku u *Unix Epoch Time (ms)* formatu
given_name	Ista vrijednost kao i kod *display_name*
sort_name	Ime kontakta korišteno u operacijama sortiranja
nickname	WhatsApp nadimak kontakta (postavljen na profilu kontakta)
company	Tvrtka (postavljena na profilu korisnika)
title	Titula (Gđa., gosp., postavljena na profilu kontakta)

Izvor: [20], [21]

Tablice koje su spomenute a sadrže podatke vrijedne za istragu su *sqlite_sequence* koja sadrži podatke o broju kontakata, te tablica *android_metadata* iz koje se mogu iščitati pojedinosti o korištenom jeziku i ostalim detaljima vezanim za interakciju Android OS-a i WhatsApp aplikacije.

U prethodno navedenim stručnim radovima navode se datoteke koje bi mogle biti od velike važnosti za početak istrage te za očuvanje integriteta i cjelovitosti podataka. WhatsApp ovisno o korisnički postavljenoj konfiguraciji periodički radi sigurnosnu kopiju svih razgovora, tj. *msgstore.db* baze podataka. Tako je na datotečnoj putanji */data/media/0/WhatsApp/Databases/* (ukoliko se pohranjuje na lokalnu memoriju uređaja) ili */mnt/sdcard/WhatsApp/Databases/* (ukoliko se pohranjuje na vanjsku memoriju, SD karticu) moguće pronaći pohranjene kriptirane sigurnosne kopije koje mogu bit korisne ukoliko je određeni sadržaj izbrisan koji bi mogao biti koristan za istragu. Pomoću sigurnosnih kopija moguće je regenerirati razgovore od i do određenog datuma što daje mogućnost za pronalazak novih i vrijednih podataka. Osim sigurnosnih kopija, WhatsApp stvara *key* (ključ) datoteku koja se koristi prilikom dekriptiranja kriptiranih sigurnosnih kopija. *Key* datoteka najčešće se nalazi na datotečno putanji */data/data/com.whatsapp/files/.*

Osim prethodno navedenih tablica, za kvalitetnu forenzičku analizu potrebno je izvršiti ekstrakciju datoteke *registration.RegisterPhone.xml* koja sadrži podatke o broju telefona koji je dodan određenom kontaktu a nalazi se na datotečnoj putanji */data/data/com.whatsapp/shared_prefs.* Datoteka *axolotl.db* sadrži kriptografske ključeve i ostale podatke potrebne za identifikaciju korisničkog profila, dok datoteka *chatsettings.db* sadrži podatke o konfiguraciji same aplikacije.

U tablici 4 navedene su datotečne putanje određenih mapa ili podmapa koje mogu sadržavati podatke poput fotografija, video i audio zapisa, log zapisa i ostalo, te kratki opis određene mape tj. datoteka koje su pohranjene u istoj.

Tablica 4. Popis datoteka od interesa za forenzičku analizu WhatsApp aplikacije

PUTANJA	OPIS
/data/media/0/WhatsApp/Media/WhatsApp Images/	Sadrži prenesene slikovne datoteke
/data/media/0/WhatsApp/Media/WhatsApp Voice Notes/	Sadrži audio zapise u *.opus* formatu
/data/data/com.whatsapp/cache/Profile Pictures/	Sadrži slikovne datoteke: slike profila kontakata
/data/data/com.whatsapp/files/Avatars/	Sadrži slikovne datoteke: ikone slike profila korisnika u *.jpeg* ili *.jpg* formatu

/data/data/com.whatsapp/files/Logs/	Sadrži *log* zapise sustava i *log* zapise programa za stvaranje sigurnosne kopije
/data/media/0/WhatsApp/Media/WhatsApp Audio/	Sadrži primljene audio zapise
/data/media/0/WhatsApp/Media/WhatsApp Audio/Sent/	Sadrži poslane audio zapise
/data/media/0/WhatsApp/Media/WhatsApp Images/	Sadrži primljene slikovne datoteke
/data/media/0/WhatsApp/Media/WhatsApp Images/Sent/	Sadrži poslane slikovne datoteke
data/media/0/WhatsApp/Media/WhatsApp Video/	Sadrži primljene video zapise
/data/media/0/WhatsApp/Media/WhatsApp Video/Sent/	Sadrži poslane video zapise
/data/media/0/WhatsApp/Media/WhatsApp Profile Photos/	Sadrži slikovne datoteke koje prikazuju slike profila korisnika čiji uređaj je predmet istrage

Izvor: [20], [21]

Naravno, uvijek je potrebno voditi računa ima li uređaj koji je dio istrage implementiranu vanjsku pohranu koja može sadržavati vrijedne podatke, ali u ovom diplomskom radu uređaj nad kojim će se vršiti postupci forenzičke analize nema implementiranu vanjsku pohranu što olakšava sami proces ekstrakcije i analize podataka.

4. Hardverski i softverski alat mobilne forenzike

Okosnica ovoga diplomskog rada je opisati i prikazati postupke i procese koji opisuju forenzičku analizu digitalnog uređaja. Sve većim tehnološkim napretkom termin „digitalni uređaj“ postao je dio svakodnevnog života što rezultira visokom razinom ovisnosti tj. potrebe za korištenjem istih. Iz tog razloga sve je veća potreba za provođenjem forenzičke analize nad digitalnim uređajima kao što su pametni telefoni, tableti, prijenosna računala, nosivi uređaji, i ostalo. Klasifikacija forenzičke analize biti će opisana u petom poglavlju, dok će se ovo poglavlje bazirati na forenzičkom alatu. Forenzički alati u osnovnoj podjeli se mogu klasificirati na hardverske alate i softverske alate. Pod hardverske alate ubrajaju se prijenosna računala, čitači, blokatori pisanja, adapteri, Faradeyeve vrećice, kablovi, itd., dok se pod softverske alate ubrajaju računalni programi koji imaju mogućnost prikupljanja i analize digitalnih dokaza te izrade odgovarajućih izvještaja kako bi prikupljeni dokazi bili vjerodostojni u nekom privatnom ili sudskom procesu.

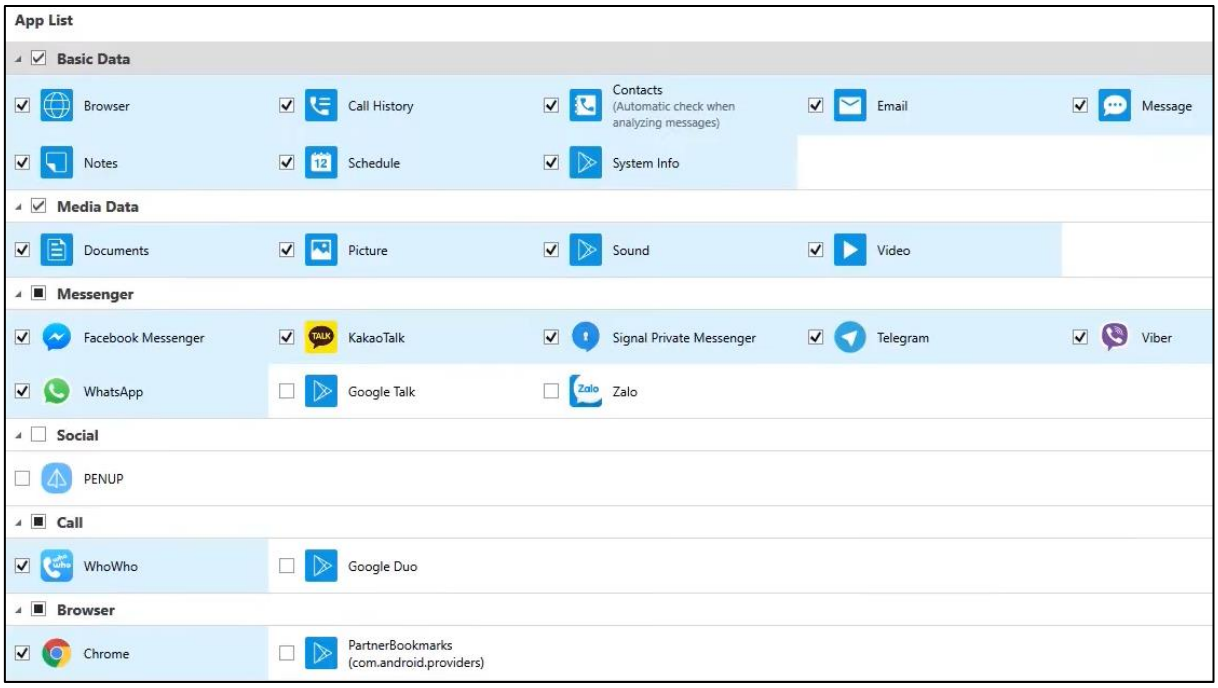
U ovom diplomskom radu korišteni su softverski alati tvrtke Hancom koja je jedna od vodećih tvrtki na tržištu. U nastavku su opisani alati koje tvrtka Hancom ima u ponudi, uz napomenu da Hancom nudi mogućnosti obuke i certificiranja istražitelja, tečajeve mobilne forenzike za istražitelje i revizore, podršku forenzičke službe te forenzičko laboratorijsko okruženje u kojemu provode istraživanja. Softverski alati koje nudi Hancom su: MD – LIVE, MD – NEXT, MD – RED, a hardverski alati su: MD – BOX, MD – READER, MD – MR. Osim toga Hancom nudi i nekoliko paketa koji objedinjuju softverske i hardverske alate kao što su: MD – RUGGED, MD – PORTABLE, MD – ACADEMY.

4.1 Softver za forenzičku analizu

4.1.1 MD – LIVE

Softver za forenzičku analizu mobilnih uređaja koji je pogodan za terensku primjenu pošto ima mogućnosti ekstrakcije i analize podatak uživo na mobilnom uređaju. Podržava logičko izdvajanje podataka i brzu analizu istih što istražitelju uvelike olakšava i ubrzava posao. Uz to, nudi mogućnost selektivnog prikupljanja dokaza bez kršenja privatnosti, snimanje zaslona uređaja i zrcalnog zaslona pametnih telefona te snimanje forenzičkog postupka eksternom forenzičkom kamerom.

Opcija selektivnog izdvajanja i analize podataka o dokazima daje istražitelju mogućnost da označi dokaze za koje misli da su od veće važnosti za slučaj kako bi ih kasnije mogao analizirati, što je i prikazano na slici 4.



Slika 4. Selektivno izdvajanje podataka u MD-LIVE softverskom alatu

Izvor: Autor (osobni primjer)

Naravno ne smije se izostaviti zakonska regulativa koja istražitelja ograničava na analizu samo onih dokaza koji su važni za slučaj ili onih vrsta podataka koji su navedeni u nalogu. Selektiranje podataka doprinosi zaštiti osobnih podataka koji su pohranjeni na uređaju te omogućuje skeniranje programa instaliranih na uređaju koji su vremenski dugo i često korišteni od strane korisnika.

Zrcaljenje zaslona i udaljena kontrola zaslona pametnog telefona istražitelju osigurava pristup sučelju uređaja ukoliko je došlo do puknuća (neispravnog rada) samog zaslona ili ukoliko istražitelj ne želi izvršavati direktno operacije na samom uređaju. Zrcaljeni zaslon se može snimiti i pohraniti kao dokaz u istrazi.

Karakteristike koje još više olakšavaju rad na softveru podrazumijevaju olakšano i intuitivno korisničko sučelje, automatsko otkrivanje modela uređaja u većini slučajeva te automatizirana analiza podataka nakon procesa prikupljanja.

Ono što je opcionalno u ovom modelu je vanjska samostojeća kamera koja služi kako bi se fotografirali dokazi ili snimile radnje tijekom postupka istrage, karakteriziraju je hardversko automatsko fokusiranje i podloga koja onemogućava refleksiju svjetlosti.

Izvještaje je moguće generirati u PDF ili Excel formatu, s mogućnošću generiranja „Dokumenta svjedoka“, uz podršku raznih HASH algoritama poput: MD5, SHA1/224/256/384/512, RIPEMD 128/160/256/320.

4.1.2 MD – NEXT

Forenzički softverski alat čija je funkcija ekstrakcija podataka sa raznih mobilnih i digitalnih uređaja. Podržava fizičku i logičku ekstrakciju za operativne sustave poput Android OS-a, iOS, Windows OS-a, Tizen OS-a, i ostalih operativnih sustava mobilnih uređaja. MD - NEXT podržava ekstrakciju podataka sa MD - READER-a (Chip-off memorija), MD – BOX-a (JTAG sučelje), USIM čitača, SM memorijskih čitača, OS backup protokola i ostalih novijih ekstrakcijskih metoda.

Ističe se po tome što se karakterizira kao kompletni alat za prikupljanje podataka mobilnih uređaja, što podrazumijeva kompatibilnost s raznim proizvođačima pametnih telefona i svim mogućim modelima istih tih proizvođača (Samsung, Apple, LG, HTC, ZTE, itd.). Osim toga ima podršku za kineske proizvođače mobilnih uređaja poput Huawei, Xiaomi, Oppo, Vivo i ostali. Podrška IoT uređaja, AI zvučnika, pametnih televizora i dronova svrstava MD – NEXT softverski alat uz bok ostalim renomiranim forenzičkim alatima.

Karakteristike naprednog fizičkog prikupljanja podataka istražitelju omogućavaju korištenje metoda poput Bootloadre-a, Fastboot-a, MTK, QEDL, izvačenje Android Rooted slike, iOS fizičke ekstrakcije, DL, JTAG, Chip-off, prikupljanja podataka sa SD memorijske kartice i ostalih dodatnih memorijskih medija. ADB Pro ekstrakcijska metoda podržava prikupljanje podataka koristeći se ranjivostima pametnog mobilnog uređaja koji se pokreće na Android OS-u.

Logička ekstrakcija podataka naprednih značajki podrazumijeva podršku za Android Live ekstrakciju, MTP, cjeloviti *backup* iOS sistemskih datoteka, Vendor *backup* protokola, lokalnih *backup*-ova i USIM-a. Što se tiče iPhone uređaja, dodatno podržava iOS *keychain* ekstrakciju, logičku ekstrakciju svih iPhone modela sve do XS i XR te dekriptiranje sigurnosnih kopija podataka za najnoviju verziju iOS uređaja.

Što se tiče Android OS, podržava fizičko prikupljanje podataka kroz sve premosnice zaključavanja (KNOX, FRP/OEM, zaključavanje zaslona) za sve Samsung uređaje S/J/A/Note serija. Istražitelj ima opciju korištenja ADB Pro funkcije koja omogućava ekstrakciju protokola sigurnosnih kopija Samsung, LG i Huawei uređaja. Lokalna ekstrakcija sigurnosnih kopija podržana je za Huawei, Xiaomi, Oppo i Gionee uređaje. Potrebno je napomenuti kako je omogućena i fizička ekstrakcija Japanskih modela poput Sharp-a i Sony-a. Osim toga MD – NEXT ima mogućnost korisničkog definiranja metoda ekstrakcije podataka koje služe za prikupljanje podataka s modela uređaja koji nisu prethodno nabrojan, tj. manje su poznati i korišteni. Nezaobilazno je napomenuti kako MD – NEXT softverski alat ima mogućnost prikupljanja podataka sa Google pogona u oblaku.

Kao i MD – LIVE, podržava selektivno prikupljanje podataka, svrstavajući ih po vrsti datoteke, kategoriji i aplikaciji. MD – NEXT automatski prepoznaje i dekriptira particijske tablice i kriptirane particije, kao i povezivanje više slika poput MDF-a i binarnih datoteka. Kao i MD – LIVE ima podršku za većinu HASH algoritama.

Potrebno je napomenuti kako ima mogućnost podrške pregleda prikupljenih podataka u hex pregledniku te je dodatna opcija zvučnog obavještavanja istražitelja o promjeni statusa ekstrakcije.

Generirana izvješća sadrže informacije poput HASH vrijednosti, vremena istrage, metode korištene u istrazi i nazive datoteka nad kojima je provedena analiza. Također ima opciju generiranja izdvojene liste datoteka koja sadrži HASH vrijednosti pojedine datoteke kako bi se naknadno mogao utvrditi integritet podataka.

4.1.3 MD – RED

Forenzički softverski alat koji služi za obnovu, dekodiranje, dekriptiranje, vizualizaciju i generiranje izvješća prikupljenih podataka sa mobilnih uređaja. Podržava analizu podatak prikupljenih pomoći MD – NEXT ili nekih drugih alata. Podržava operativne sustave raznih proizvođača čime je omogućena forenzička analiza mnogih pametnih telefona i drugih raznovrsnih digitalnih uređaja.

Specificiran je za oporavak i analizu raznih datotečnih sustava poput: FAT 12/16/32, exFAT, NTFS, ext3/4, HFS+, EFS, YAFFS, FSR, XSR, F2FS, VDFS, XFS, DVR datotečne sustave (Dahua i Hikvision) te datotečne sustave crnih kutija (TAT).

Vezano za analizu pametni mobilnih uređaja, MD – RED ima mogućnost analize preko 2000 aplikacija, uključujući i neke nove aplikacije. Neke od aplikacija i datoteka koje MD – RED može analizirati su; razne multimedijske datoteke snimljene samim uređajem, popis poziva, SMS/MMS poruke, sadržaj adresara, povijest *web* preglednika, društvene aplikacije, kartografske i navigacijske aplikacije, aplikacije medicinskog sadržaja, aplikacije Internet bankarstva i ostalo.

MD – RED istražitelju omogućava paralelnu analizu kroz višejezgreni proces i dešifriranje podataka pohranjenih u šifriranim porukama raznih aplikacija. Dubinska analiza aplikacija za razmjenu poruka podrazumijeva dekodiranje i oporavak podataka generiranih u aplikacijama poput WhatsApp-a (dešifriranje većeg broja sigurnosnih kopija datoteka), WeChat-a (analiza nekoliko računa i *rainbow* tablica), Skype, Facebook messenger, Telegram, Wickr, QQ, Kakaotalk, Line, Zalo, Viber, Snapchat i ostalih aplikacija sličnih funkcionalnosti.

Uređaj je moguće otključati na nekoliko načina koji se baziraju na dekodiranju uzoraka zaključavanja, PIN-a i lozinke, a time se istražitelju omogućava analiza podataka pomoću sučelja samog uređaja.

Oporavak i analiza multimedijskog sadržaja karakteristična je za ovaj alat iz razloga što MD – RED oporavlja izbrisane ili oštećene video datoteke, omogućuje pretraživanje audio datoteka poput Samr, AUD, QCP, SILK na MP3, AMR i WAV, uz to podržava reprodukciju QCP datoteke i SILK audio datoteka.

Kako bi istražitelj ima detaljniji i realniji uvid u prikupljene podatke, MD – RED ima nekoliko ugrađenih preglednika. SQLite preglednik baze podataka, HEX preglednik, PList preglednik, preglednik dokumenata (tekst, XML, PDF, MS Office, ZIP datoteke, izvršne datoteke, kriptirane datoteke), preglednik galerije slika, te reproduktor video i audio sadržaja.

Napredne opcije filtriranja podataka imaju mogućnost segmentacije podataka ovisno o vrsti datoteke, vremenu nastanka datoteke i ključnim riječima, a kao dodatak moguće je ključne riječi registrirati za daljnji postupak istrage, označiti rezultate dobivene filtriranjem i naravno ukloniti rezultate. Korisnički definirana analiza podataka podržava Python IDE skripte koje se pokreću u Python editoru za napredne korisnike, što kao rezultat daje generiranje koda, izvršavanje i otklanjanje pogrešaka.

Vizualizacija analiziranih datoteka podrazumijeva prikaz GPS podataka prikupljenih datoteka (slika, video i audio zapisa) što je prikazano na slici 5, lokacija baznih stanica, izvanmrežne i mrežne karte u 3 razine (grad-regija-država), vremenske linije koja je od izuzetne važnosti za istragu, linkova koji povezuju društvene odnose među osobama koje su predmet istrage, komunikacijskih veza između osoba što istražiteljima koristi u daljnjem postupku istrage te povijest *web* preglednika koja omogućava pregled sadržaja kojeg je osumnjičeni pretraživao (područje interesa korisnika čiji je uređaj predmet istrage).

4.2 Hardver za forenzičku analizu

4.2.1 MD – BOX

Jedan od tri HANCOM forenzičkih alata koji spada u kategoriju hardverskih alata. Koristi se u slučajevima kada je potrebno prikupiti podatke na fizički način, tj. kada je potrebno povezati određeni mobilni uređaj za kojega je istražitelj dobio nalog ali je onemogućeno korištenje uređaja ili je uređaj mehanički oštećen. MD – BOX je forenzički alat, prikazan na slici 5, koji prikuplja podatke direktnim povezivanjem na matičnu ploču mobilnog uređaja pomoću JTAG sučelja, nakon čega se podaci mogu pregledati u MD – NEXT programskom alatu.

Slika 5. MD - BOX forenzički alat

Izvor: Autor (osobni primjer)

Neke od naprednih značajki alata podrazumijevaju automatsko skeniranje particija, ekstrakciju određene (željene) particije, ekstrakciju bez referentnog napona, DMA (engl. *Direct Memory Access*) ekstrakciju te mogućnost nastavka ekstrakcije od posljednje točke prekida.

Uz podršku desetak HASH algoritama poput MD5 i SHA256, MD – BOX ima mogućnost blokiranja pisanja kako bi se sačuvao integritet podataka, tj. dokaza. Maksimalna brzina ekstrakcije iznosi 1MB/sek što bi značilo da mobilni uređaj sa memorijom od 128 GB ekstrahira za 37 sati ukoliko je memorijski prostor napunjen do kraja. Podržava procesore poput MSM6xxx, MSM7xxx, APQ, Exynos, OMAP, Cortex-A i ostali.

MD – BOX kompatibilan je sa FPCB setovima kabela ali uz to omogućava ručno povezivanje lemljenjem što istražitelju daje veću šansu za ekstrakciju bitnih podataka. Podatke sprema kao MDF slikovnu datoteku uz pomoć MD – NEXT softvera.

U nastavku ovoga seminarskog rada opisati će se proces povezivanja mobilnih uređaja s FPCB i PCB kablovima. Opis će biti popraćen slikama procesa kojeg provodi certificirani istražitelj.

4.2.2 MD - MR

Pošto digitalna forenzika podrazumijeva specifične postupke prilikom procesa prikupljanja podataka, potrebni su i specifični alati kako bi istražitelj uspješno došao do neoštećenog ili što manje oštećenog medija na kojemu su pohranjeni podaci, tj. digitalni dokazi. Ukoliko je uređaj ozbiljno oštećen, slomljen, zapaljen ili tretiran nekim abrazivnim sredstvima, tada je klasična ekstrakcija koja podrazumijeva kabelsko povezivanje onemogućena. MD –MR je paket hardverskih forenzičkih alata (uređaja) koji služe za odvajanje memorijskih čipova sa matične ploče mobilnog ili nekog drugog digitalnog uređaja. MD – MR se koristi prije nego što će istražitelj medij pohrane podvrgnuti Chipp-off metodi ekstrakcije, koja će biti opisana u sljedećem poglavlju.

MD – MR paket sastoji se od osnovnih uređaja za ručno uklanjanje memorijskih čipova, što podrazumijeva 5 *flash* eMMC/ eMCP memorijskih utičnica kompatibilnih s MD-READER-om, puhalicu za demontažu, stanicu za ručno lemljenje, usisavač dima, mikroskop (3,5 do 180 puta povećanje i oprema za osvjetljenje) te digitalni mikroskop s HDMI i USB ulazima.

Od dodatnih uređaja sadrži preradnu stanicu za male PCB (BK-350S) koja je optimizirana za rad na mobilnim uređajima, sušilicu za PCB ploču i mali digitalni uređaj (rg-202) koji održava stabilnu temperaturu kako bi se spriječilo uništenje čipa te sigurnosnu kutiju za mobilni uređaj koja ima mogućnosti punjenja uređaja, fizičke pohrane samog uređaja, sterilizaciju uređaja i digitalni sustav zaključavanja kutije.

4.2.3 MD – READER

Koristi se za izdvajanje podataka direktno s memorijskog čipa, poznato kao chip-off metoda ekstrakcije koja se rijetko koristi pošto je to posljednje što istražitelj koristi kao ekstrakcijsku metodu, razlog je to što ta metoda može trajno uništiti memorijski čip, a samim time i podatke koji su pohranjeni na njemu. Memorijski čip umeće se u jednu od 15 mogućih memorijskih utičnica, nakon toga može se izvršiti ekstrakcija podataka u MD – NEXT softverskom alatu pod kategorijom „Chip-off“.

Uz mogućnost ekstrakcije memorijskih čipova, MD – READER nudi mogućnost ekstrakcije memorijskih kartica, s obzirom na to MD – READER sadrži utore za SD karticu, Micro i mini SD karticu. Osim toga, podržava automatsko i selektivno skeniranje particija s maksimalnom brzinom ekstrakcije od 12MB/s.

Kako se ne bi narušio integritet podataka prilikom ekstrakcije, MD – READER podržava blokator pisanja te 10 različitih HASH algoritama. Pomoću MD – NEXT softvera podatke pohranjuje kao MDF slikovnu datoteku.

5. Ekstrakcija podataka aplikacija za trenutačnu razmjenu poruka

Kao što je već u drugom odlomku navedeno, podaci mobilnih terminalnih uređaja imaju veliki značaj u procesu forenzičke analize i same kriminalističke istrage koja se provodi nad osumnjičenikom. Iz tog razloga veliku pozornost potrebno je dati metodama i pravnim regulativama koje opisuju i ograničavaju istražne procese i postupke prilikom forenzičke analize uređaja. Naime jedna od najpoznatijih i najkorištenijih metoda forenzičke analize mobilnih terminalnih uređaja je *Cellular Phone Evidence Extraction Process* koju je izdao SANS institut. Metoda podrazumijeva skup smjernica, postupaka i definiranih dokumenata koji istražitelju omogućuju osiguranje konzistentnosti dokaza koji su u obliku podataka ekstrahirani iz uređaja.

Ova metoda forenzičke analize mobilnih terminalni uređaja počiva na devet referentnih faza koje istražitelju pružaju očuvanje integriteta podataka uz istražiteljevu preciznu i opreznu manipulaciju mobilnim uređajem i ekstrakcijskim alatima i detaljno vođenje lanca posjeda dokaza. U nastavku su navedene faze po redoslijedu od početne do završne od kojih se neke mogu i moraju ponavljati.

Faze SANS referentne metodologije:

1. Uvođenje dokaza

Podrazumijeva dokumentaciju za unos dokaza (uređaja) u lanac posjeda dokaza, obradu zahtjeva koji je generiran od strane privatne ili pravne osobe koja potražuje proces forenzičke analize. Navode se opće informacije o vrsti podataka i informacija koje podnositelj zahtjeva traži. U ovoj fazi razvijaju se specifični ciljevi istrage kojima se žele prikupiti zahtijevani dokazi koji će biti određene razine integriteta. Istražitelju nije u interesu prikupiti podatke koji nisu navedeni u zahtjevu jer time smanjuje integritet i vjerodostojnost željenih podataka.

2. Identifikacija

Prilikom svakog postupka ispitivanja mobilnog terminalnog uređaja istražitelj mora utvrditi sljedeće:

a. Zakonsko pravo za ispitivanje uređaja – istražitelj prije početka istrage utvrđuje i dokumentira pravna ovlaštenja i ostala ograničenja pretrage koja su navedena u zahtjevu:
    i. Ukoliko se uređaj istražuje na osnovu naloga, u tom slučaju istražitelj mora biti svjestan ograničenja koja su postavljena u nalogu.
    ii. Ukoliko se uređaj istražuje na osnovu pristanka, ograničenja moraju biti specifično definirana i preventivno provjerena netom prije početka istražnog procesa.
    iii. Ukoliko se uređaj istražuje u slučaju kriminalne istrage u kojoj je korisnik uhapšen, tada istražitelj mora biti posebno oprezan iz razloga što je trenutna sudska praksa u ovom području posebno problematična i sklona učestalim izmjenama i dopunama zakona.

b. Ciljeve istrage,
c. Informacije o marki, modelu i identifikacijskim oznakama,
d. Unutarnju i vanjsku memorijsku pohranu,
e. Ostale izvore potencijalnih dokaza, [3]

3. Priprema

Odabir odgovarajućeg forenzičkog alata s obzirom na podatke i uređaj koji se istražuje, odabir odgovarajuće metode ekstrakcije podataka, odabir i testiranje potrebnih kablova za povezivanje mobilnog uređaja i forenzičke opreme, pripremanje medijske pohrane od strane istražitelja prepisivanjem nulama, testiranje i provjera softverskih forenzičkih alata, itd. S obzirom na cilj istrage, resursa dostupnih organizaciji koja vrši istragu, vrste mobilnog uređaja i činjenici o prisutnosti vanjske memorijske pohrane odabire se prikladni forenzički alat. U tablici 2 navedeni su forenzički alati s obzirom na vrstu komunikacijske tehnologije i vrstu pohrane.

4. Izolacija

Pošto većina mobilnih uređaja ima implementirano barem dvije vrste mobilne komunikacijske tehnologije, potrebno je na odgovarajući način izolirati uređaj od vanjskog utjecaja elektromagnetskog zračenja kako bi se onemogućila manipulacija, izmjena i brisanje podataka od strane neovlaštenog ili zlonamjernog korisnika. Izolaciju je moguće ostvariti pohranjivanjem uređaja u Faradey-eve vrećice, kutije ili kaveze, te je moguće ometanje signala mobilnih komunikacijskih tehnologija pomoću signal *jammer*-a.

5. Procesiranje

Postupak analize koji podrazumijeva korištenje prethodno odabranog alata uz praćenje definiranih ciljeva i zakonskih ograničenja. Korištenjem odgovarajuće metode ekstrakcije podataka istražitelj dobiva uvid u prikupljene podatke koji ukoliko im se zadovolji kriterij integriteta postaju dokazi. Pošto mobilni uređaj prilikom rada intenzivno komunicira s vanjskim pohranama potrebno je zasebno ekstrahirati mobilni uređaj (unutarnja memorija), vanjsku memorijsku pohranu (npr. microSD kartica) i SIM krticu, kako ne bi došlo do neželjene promjene podataka.

6. Verifikacija

Postupak potvrde prikupljenih podataka od strane istražitelja kako bi podaci bili vjerodostojni i prihvatljivi na sudu. Izvršava se na tri uobičajena načina:

a. Usporedba ekstrahiranih podataka s podacima koji su pohranjeni na uređaju,
b. Upotrebom nekoliko raznovrsnih forenzičkih alata i usporedba dobivenih rezultata,
c. Upotrebom *hash* vrijednosti (*hash* – jedinstveni identifikator datoteke koji mijenja svoju vrijednost u slučaju modifikacije datoteke).

7. Dokumentiranje

Provodi se tijekom cijelog procesa istrage kroz lanac posjeda dokaza i ostale bitne izvještaje koji opisuju postupke provedbe istrage. Često se koriste unaprijed formulirani predlošci koji sadrže osnovne podatke poput: datum i vrijeme početka istrage, fizičko stanje uređaja, fotografije vanjskog stanja uređaja i popratne opreme, status uređaja u trenutku primitka, model uređaja, korišteni alati, ekstrahirani podaci, itd.

8. Prezentacija

Jedna od bitnijih faza iz razloga što mora dati jasan prikaz dobivenih rezultata sudskom osoblju i odgovornoj osobi bez obzira na njihovu tehničku pismenost. Nerijetko se koriste prikazi zaslona koji daju informacije o sadržaju određene aplikacije, poruke ili galerije slika.

9. Arhiviranje

Čuvanje prikupljenih podataka i uređaja tijekom i nakon završenog sudskog procesa kako bi se zadovoljilo trenutnim i budućim zahtjevima od strane suda. Ukoliko postoji mogućnost podatke je potrebno pohraniti u standardnim formatima i na standardnim medijima kako bi se omogućilo lakše pristupanje podacima u budućnosti.

U prethodno navedenim fazama objašnjen je proces provedbe forenzičke analiza nad mobilnim terminalnim uređajem koji podrazumijeva sve najnovije metode i procese same forenzike mobilnih uređaja. Uloga istražitelja u ovom procesu je da pravovremeno detektira ograničenja koja su mu zakonom propisana te ograničenja koja je propisalo nadležno tijelo. Veliki izazov u ovom procesu je ekstrakcija podataka iz razloga što je postupak separacije traženih podataka otežan iz razloga što današnji mobilni terminalni uređaji prikupljaju enormnu količinu podataka što potkrepljuje činjenica da danas ima više terminalnih uređaja nego stanovnika na svijetu.

5.1 Metode ekstrakcije

Podrazumijeva 5. fazu SANS metodologije koja opisuje sami proces ekstrakcije tj. prikupljanja podataka s uređaja koji je naveden u nalogu kako bi se omogućila analiza prikupljenih podataka. Ciljevi koji su zadani u prvoj fazi određuju koja će se metoda ekstrakcije primjenjivati kako bi se prikupila dovoljna količina korisnih podataka. Najjednostavnije metode poput ručne ekstrakcije prikupljaju malu količinu vrijednih podataka ali su vremenski najkraće, dok metode poput JTAG-a zahtijevaju stručnost istražitelja i velike forenzičke resurse koji ponekad nisu dostupni. Ukoliko jednostavne metode nisu dovoljno efikasne koriste se kompleksnije metode koje zahtijevaju više vremena, te uz to zahtijevaju omogućavanje pristupa tvorničkim podacima što je omogućeno *root*-anjem uređaja.

U nastavku ovoga diplomskog rada navedene su metode ekstrakcije podataka s mobilnih terminalnih uređaja koje su trenutno dostupne i omogućavaju uz pravilnu manipulaciju integritet podataka.

Ručna ekstrakcija

U prošlosti podrazumijeva ručno prepisivanje podataka (imenik, poruke, zabilješke) s mobilnih uređaja, dok se u današnje vrijeme pametnih mobilnih uređaja ta metoda svodi na sekvencijalno listanje podataka na mobilnom uređaju putem ekrana dok sve te korake i snimke zaslona evidentira posebna forenzička kamera visoke rezolucije. Ukoliko mobilni uređaj sadrži veću količinu podataka ova metoda traje predugo, osim toga ova metoda ne omogućava prikupljanje podataka o datotečnim sustavima i *log* zapisima.

Logička ekstrakcija

Glavna karakteristika je ta da se mobilni uređaj povezuje pomoću originalnog sučelja s istražiteljevim računalom kako bi se omogućio prijenos podataka. Povezivanje mobilnog uređaja i forenzičkog alata moguće je pomoću USB kabela, RJ-45 kabelske izvedbe, infracrvene ili Bluetooth tehnologije. Nakon što se uređaj poveže s računalom, računalo na uređaj šalje niz naredbi koje uređaj interpretira i povratno šalje odgovore koji se tada konvertiraju u čitljive podatke, dokaze. Ovakva vrsta ekstrakcije temelji se na programskim sučeljima pojedinog mobilnog uređaja što bi trebalo istražitelja potaknuti na korištenje *root* pristupa uređaju kako bi prikupio veću količinu podataka. Dvije su osnovne vrste ovakve metode prikupljanja podataka;

- Agentski temeljena ekstrakcija koja podrazumijeva instalaciju određene aplikacije (agenta) na mobilni uređaj kako bi se prikupili podaci te brisanje agenta nakon završetka ekstrakcije,
- Ekstrakcija korištenjem ADB naredbi koja podrazumijeva aktivaciju *USB debugging* moda kako bi se omogućila komunikacija mobilnog uređaja i forenzičkog alata.

Datotečna ekstrakcija

Po poretku na piramidalnoj tablici metoda ekstrakcije nalazi se između logičke i fizičke metode iz razloga što dohvaća sve datoteke koje su pohranjene na memoriji uređaja čiji se dio smatra zauzetim, dio klastera koji nije ispisan može se pročitati. Omogućava prikupljanje podataka poput: baze podataka aplikacija, sistemskih podataka, log zapisa, povijesti pretraživanja, itd.

Fizička ekstrakcija

Predstavlja naprednu metodu koja u nekim slučajevima podrazumijeva fizičko rastavljanje uređaja kako bi se došlo do memorijskih čipova te omogućilo prikupljanje podataka *bit-by-bit,* što podrazumijeva analizu cjelokupnog memorijskog prostora, kako unutarnje tako i vanjske memorije. Zapis je u binarnom formatu što istražitelju uvjetuje korištenje određenih softverskih alata kako bi se uspješno dekodirao prikupljeni sadržaj. Ova metoda sadrži tri različite kategorije ekstrahiranog sadržaja:

1. Logički sadržaj koji je dostupan korištenjem korisničkog interfejsa
2. Obrisani i skriveni sadržaj
3. Sadržaj koji mobilni uređaj generira bez korisnikove interakcije

Jedna od najvećih beneficija ove metode je ekstrakcija izbrisanih podataka što u tijeku istrage može dovesti do značajnih promjena. Ukoliko je omogućena metoda neinvazivne fizičke ekstrakcije, tada se koriste metode; *client, ADB, bootloader* i *forensic recovery partition,* što istovremeno ne zahtijeva rastavljanje mobilnog uređaja. Invazivna fizička ekstrakcija podrazumijeva rastavljanje mobilnog uređaja kako bi se pristupilo SoC-u, matičnoj ploči i memorijskim modulima. Invazivne metode podrazumijevaju JTAG, chip-off, ISP-eMMC i Micro Read načine ekstrakcije.

- JTAG – *Joint Test Action Group* predstavlja udrugu elektroničkih industrija čija je zadaća dizajniranje i nadziranje proizvodnje tiskanih pločica. Ovom metodom omogućava se napredni način ekstrakcije podataka koji uključuje povezivanje mobilnog uređaja i forenzičkog *reead*-era pomoću FPCB konektora što je i prikazano na slici 2.
- ISP-eMMC - ukoliko ne postoji odgovarajuće sučelje za povezivanje FPCB konektora, tada se koristi PCB konektor koji je prikazan na slici 3. U tom slučaju istražiteljev zadatak je da se precizno i detaljno informira o rasporedu odgovarajućih konektora kako bi uspješno zalemio odgovarajuće žice na odgovarajuće pinove koji se nalaze na matičnoj ploči.
- Chip-off - metoda koja se zasniva na postupcima fizičkog izdvajanja memorijskog čipa s matične ploče određenim alatima koji pod točno definiranom temperaturom zagrijavaju čip (niti previše da ga unište, niti premalo da ga ne odleme), koji se nakon detaljnog čišćenja polaže u memorijsku utičnicu koja se zatim povezuje s forenzičkim alatom koji prikuplja podatke.
- Micro Read – metoda koja se jako rijetko koristi u forenzičkoj analizi, koriste ju samo nadležne državne vlasti kako bi došle do podataka s fizički uništenih uređaja jakog stupnja (pregaženi, zapaljeni, potopljeni, uronjeni u kiselinu). Zasniva se na metodama koje podrazumijevaju korištenje preciznih elektroničkih mikroskopa koji s obzirom na postojeće veze u poluvodičkim materijalima u memorijskim čipovima pokušavaju rekonstruirati zapisane podatke.

U nastavku biti će opisane zakonske regulative kojih se istražitelj mora pridržavati kako bi podaci koji su prikupljeni bili vjerodostojni na sudu. Osim toga potrebno je obratiti pozornost na procese provođenja forenzičke analize od strane istražitelja.

5.2 Zakonska regulativa

Kao što je navedeno već prije u ovom diplomskom radu, proces forenzičke analize vrlo je osjetljiva i specifična radnja koja se mora odvijati pod posebnim uvjetima te mora biti rukovođena od strane stručnog osoblja kako bi se uspostavio integritet i vjerodostojnost prikupljenih podataka.

Prilikom procesa forenzičke analize mobilnog terminalnog uređaja istražitelj veliku pozornost mora pridati zakonima i propisima koji mu nalaži i specificiraju granične manipulativne procese kojih se mora pridržavati tokom cijelog trajanja istrage. Pošto je

Republika Hrvatska članica Europske unije, zakoni i uredbe koje obvezuju istražitelja obično se odnose na privatne korisničke podatke koji su pohranjeni na mobilnom uređaju.

Najpoznatija uredna takve vrste koja je prisutna u svakodnevnom životu građana EU je GDPR (engl. *General Data Protection Regulation*). Kako bi se regulirala manipulacija podataka poput metapodataka ili kolačića uvedena je Uredba o e-privatnosti čija je namjena dopuna i unapređenje GDPR-a, te proširenje trenutno aktualne Direktive o e-privatnosti kako bi se što detaljnije, preciznije i efikasnije harmonizirala i uredila pravila koja se direktno odnose na sve države članice EU-a. U nastavku teksta nabrojane su regulative i direktive koje se odnose na procese obrade osobnih podataka te garantiranje slobodne manipulacije osobnih podataka, [24]:

- Uredba 2018/1725
- Opća uredba o zaštiti podataka (EU) 2016/680
- Direktiva (EU) 2016/679
- Direktiva o e-privatnosti 2002/58/EC
- Direktiva 2000/31/EC
- Direktiva 98/34/EC

Pojavom GDPR-a omogućilo se je pravno reguliranje procesa obrade pravnih podataka što je u nekim slučajevima rezultiralo ukidanjem nekih odredbi poput sigurnosnih obveza iz članka 4 Direktive o e-privatnosti. Pošto članak 15. Direktive o e-privatnosti i članak 23. GDPR-a ne propisuje posebne odredbe o postupcima i pravima zadržavanja podataka, države imaju mogućnost samostalno odrediti ograničenja za takve načine manipulacije podacima. U slučaju kada država članica stvaraju nacionalne okvire za zadržavanje podataka moraju uzeti u obzir da su u skladu s pravima Unije, te moraju uzeti u obzir sudske prakse prilikom tumačenja Direktive o e-privatnosti i Povelje o temeljnim pravima. Uredba 2018/1725 donesena od strane Europskog parlamenta i Vijeća 18. listopada 2018. godine govori o zaštiti osoba u svrhu obrade osobnih podataka od strane institucijskih tijela, ureda i agencija Unije. Pravo na zaštitu osobnih podataka svake individue (osobe) propisano je člankom 8. stavkom 1. Povelje o temeljnim pravima Europske unije, člankom 16. stavkom 1. Ugovora o funkcioniranju Europske unije (UFEU), te člankom 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda. Direktiva 2016/680 i GDPR usvojeni 27. travnja 2016. godine utvrđuje posebna pravila o zaštiti fizičkih osoba u smislu obrade osobnih podataka te osigurava slobodno kretanje osobnih podataka fizičke osobe unutar Unije u razini pravosudnog sustava i međunarodne suradnje policijskih službenika, [24].

Nezaobilazno je napomenuti OLAF (engl. *European anti-fraud office*) čija je zadaća otkrivanje prijevara i ostalih ilegalnih aktivnosti koje bi mogle utjecati na financijski interes Europske unije. OLAF u sklopu pravnih osnova za provođenje digitalne forenzičke analize prema članku 4. Uredbe 883/2013, je ovlašten za kopiranje i prikupljanje podataka ili informacija s bilo kojeg medija koji je u posjedu ovlaštenih tijela, institucija, ureda ili agencija. U slučaju od rizika za nestankom ili uništavanjem medija koji pohranjuje podatke važne za istragu, OLAF ima pravo preuzeti odgovornost pohrane takvih medija s naglaskom na njihovo očuvanje i kontrolu pristupa, [24].

Još jedna od bitnih organizacija je ENISA (engl. *European Union Agency for cybersecurity*), Agencija Europske unije za kibernetičku sigurnost. Zadaća Agencije je što efikasnije provođenje propisa i zakona kako bi se osigurao veći stupanj kibernetičke sigurnosti na području Europske unije, te razvoj okvira za certificiranje kibernetičkih sigurnosnih protokola kako bi se proizvođačima i dizajnerima ICT usluga omogućila ravnopravna i efikasna natjecateljska kompetencija u okviru europskog tržišta.

Kako istražitelj ne bi povrijedio osnovna prava korisnika, tijekom istrage veliki značaj ima proces vođenja očuvanja dokaza kojega definiraju osnovne zakonske odredbe navedene u nastavku teksta, [25]:

- Zakon o elektroničkim komunikacijama – prvenstveno regulira rad operatora kao davatelja usluge, a za forenzičku analizu bitni su:
    - Članak 100. Zakona (Tajnost elektroničkih komunikacija) – zabranjeno je slušanje, pohrana ili presretanje komunikacija između korisnika, osim u slučaju članka 108. ili u postupcima koji su definirani posebnim zakonima.
    - Članak 108. Zakona (Tajni nadzor elektroničkih komunikacijskih mreža i usluga) – operatori moraju omogućiti tajni nadzor mreža i usluga, te moraju osigurati komunikaciju s tijelom nadležnim za nadzor komunikacije u skladu sa zakonom kojim je definirana nacionalna sigurnost.
- Zakon o zaštiti osobnih podataka – štiti se fizička osoba te se vrši nadzor nad procesima prikupljanja, obrade i korištenja podataka. Prema članku 6. Zakona podaci mogu biti prikupljani u svrhu s kojom je pojedinac upoznat i koja je u skladu sa Zakonom. Postoje iznimke ukoliko je riječ o povredi nacionalne ili javne sigurnosti.
- Zakon o kaznenom postupku – utvrđuje pravila kojima se osigurava da nedužni sudionici istrage ne budu oštećeni, a da se počinitelju kaznenog djela izrekne predviđena kazna ili neka druga mjera. Neki bitni članci:
    - Članak 17., kazneni postupak započinje : izdavanjem naloga o provođenju istrage, potvrđivanjem optužnice, određivanjem rasprave na temelju tužbe, donošenjem presude o izdavanju kaznenog naloga.
    - Članak 86., ukoliko se na određenom dokazu ne može donijeti sudska odluka, sudac izdvaja dokaz iz zapisnika te ga daje tajniku suda na čuvanje.
    - Članak 183., svakom sudioniku sudskog procesa može se omogućiti pristup zapisniku i referentnim dokazima koji su dio zapisnika.
    - Članak 257., definira pretragu računala i s njime povezanih uređaja čija je svrha prikupljanje, pohrana i prijenos podataka te telefonska i računalna komunikacija.
    - Članak 263., podaci se moraju predati državnom odvjetniku u originalnom i razumljivom obliku. Stvarno vremenski snimani podaci mogu se čuvati najdulje šest mjeseci.
    - Članak 332., definira posebne dokazne radnje koje podrazumijevaju prikupljanje podataka uz privremeno ograničenje ustavnih prava građana.

S obzirom na sve veći broj mobilnih terminalnih uređaja i sve veći broj aplikacija koje omogućavaju prikupljanje i manipulaciju podataka, forenzička analiza postaje vrlo složen i zahtjevan proces koji se temelji na zakonima, metodologijama i stručnim kompetencijama istražitelja.

5.3 Ekstrakcija podataka s uređaja Samsung Galaxy S9

Praktični dio ovog diplomskog rada opisan je u ovom i u sljedećem poglavlju čime se želi prikazati postupak povezivanja uređaja s forenzičkim računalom koji pokreće softverski forenzički alat tvrtke Hancom. U nastavku biti će opisan postupak pripreme uređaja, način povezivanja uređaja i forenzičkog računala te koraci koji opisuju manipulativne radnje u samom softveru. Postupak forenzičke analize uređaja Samsung Galaxy S9 u cijelosti je proveden u sklopu Laboratorija za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava.

U tablici 5 navedena je oprema i uređaji koji su korišteni tijekom provođenja procesa forenzičke analize pametnog telefona.

Tablica 5. Popis alata korištenih u procesu forenzičke analize

R. br.	Oznaka dokaza	Proizvođač	Opis	Serijski broj	Namjena
1.	Galaxy S9	Samsung	Pametni telefon (Android 10)	R58M24EV1XW	Dokaz
2.	Kabel	Samsung	USB C – USB A		Povezivanje dokaza i računala
3.	Pavilion 10	Hewlett Packard	Prijenosno računalo	5CD5425DW2	Ekstrakcija i analiza podataka
4.	Galaxy A72	Samsung	Pametni telefon (Android 10)	R58R32J7VGZ	Uređaj za evidentiranje postupaka
5.	MD – RED	Hancom	Softverski forenzički alat	Verzija: 3.7.33.1093	Analiza prikupljenih podataka
6.	MD - NEXT	Hancom	Softverski forenzički alat	Verzija: 1.90.1.1204	Ekstrakcija podataka iz dokaza

Izvor: Autor (osobni primjer)

Kako bi se osiguralo provođenje kvalitetne i cjelovite forenzičke istrage potrebno je voditi računa o kriterijima koji osiguravaju integritet prikupljenih podataka kako bi se ti podaci iskoristili kao dokazi u sudskom procesu ili neovisnoj istrazi. Kriteriji integriteta podataka nabrojani su u nastavku:

- Autentičnost – dokazi moraju biti reprezentativni i u izvornom stanju kako bi se onemogućilo osporavanje istih,
- Potpunost – Dokazi ne smiju biti modificirani i moraju biti prikazani s objektivnog stajališta,
- Pouzdanost – Mogućnost nastanka promjene nad dokazima moraju biti svedene na minimalnu vjerojatnost kako bi se osigurala visoka razina autentičnosti i istinitost

Prije početka procesa ekstrakcije podataka potrebno je navesti detaljnije informacije o samom dokazu, u ovome slučaju to je pametni telefon tvrtke Samsung, model Galaxy S9. U nastavku su opisani neki za istragu bitni dijelovi samog uređaja te su navedene osnovne identifikacijske oznake.

5.3.1 Identifikacija pametnog telefona

Zadatak ovog diplomskog rada je provedba forenzičke analize nad pametnim telefonom kako bi se izvršila analiza podataka vezanih za aplikacije koje podržavaju trenutačnu razmjenu poruka. Kako bi forenzička analiza bila vjerodostojna i cjelovita potrebno je identificirati uređaj nad kojim se vrši forenzička analiza kako bi se mogućnost povrede integriteta podataka smanjila na minimalno. U tablici 6 navedeni su osnovni identifikatori uređaja s naglaskom da su identifikatori SIM kartice izostavljeni iz razloga što uređaj tijekom forenzičke analize nije sadržavao istu.

Tablica 6. Identifikatori pametnog telefona

Identifikator	Vrijednost
Proizvođač	Samsung
Model	Galaxy S9
Serijski broj	R58M24EV1XW
IMEI (utor 1)	354663105478462
IMEI (utor 2)	354663105478460
FCC ID	A3LSMG960F
Android verzija	10
Kernel verzija	4.9.118-19869059
Knox verzija	3.4.1

Izvor: Autor (osobni primjer)

Potrebno je napomenuti kako uređaj Samsung Galaxy S9 ne sadrži nikakav oblik vanjske memorije što u startu olakšava proces ekstrakcije podataka. U sljedećem poglavlju detaljno su opisane radnje koje su provedene tijekom procesa ekstrakcije podataka.

5.3.2 Postupak logičke ekstrakcije podataka

Ekstrakcija podataka u ovom diplomskom radu izvršena je pomoću forenzičkog alata MD – NEXT tvrtke Hancom. Tijekom provedbe forenzičke analize izvršene su dvije vrste ekstrakcije, logička i fizička, što je rezultiralo većim brojem prikupljenih podataka tijekom fizičke ekstrakcije. U nastavku je opisan proces povezivanja uređaja s računalom na kojemu se nalazi forenzički alat te su detaljno opisane popratne radnje koje su izvedene s visokom razinom pažnje od strane istražitelja.

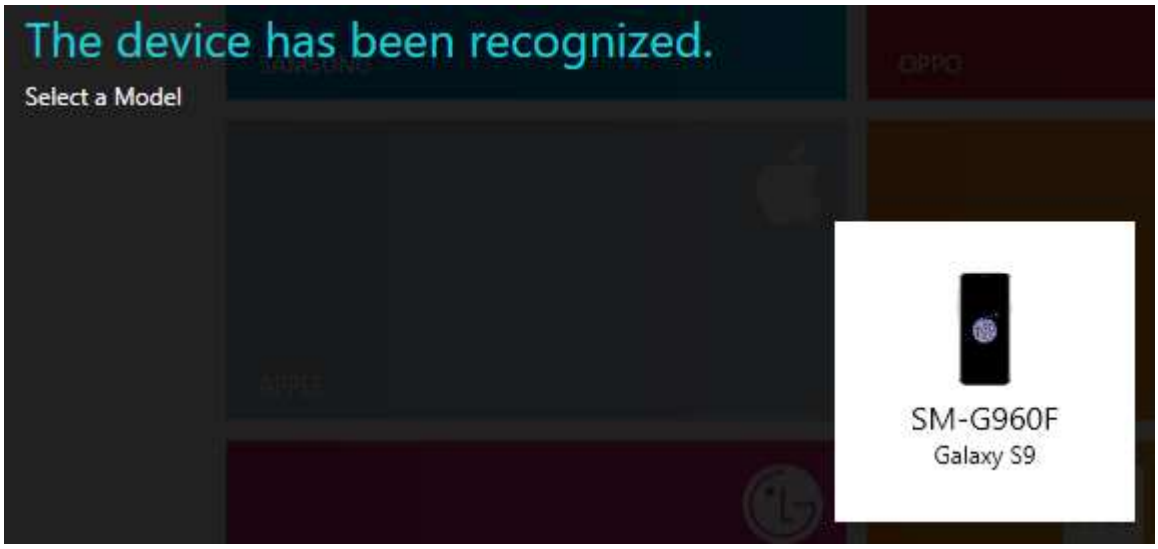
Povezivanje uređaja

Tijekom forenzičke istrage potrebno je osigurati izolaciju uređaja što je u ovom slučaju omogućeno isključenjem svih komunikacijskih tehnologija na samom uređaju (Wi-Fi, mobilna mreža, bluetooth, NFC), čime se osigurava nepromjenjivost podataka pohranjenih na uređaju.

Nakon što je uređaj izoliran potrebno ga je povezati s računalom putem odgovarajućeg USB kabela koji se sastoji od USB C konektora koji se povezuje na uređaj i USB A konektora koji se povezuje s računalom (na USB 3.0 sučelje). Obavezno je napomenuti kako kabel za povezivanje ne smije imati nikakva oštećenja kako tijekom ekstrakcije ne bi došlo do prekida veze između uređaja i računala.

Automatsko prepoznavanje uređaja

Nakon što je uređaj uspješno povezan s računalom, u alatu MD – NEXT pokreće se automatska pretraga modela pametnog telefona, što se može izvršiti i ručnom pretragom. Nakon što je uređaj uspješno prepoznat, potrebno je odabrati uređaj klikom na ikonu što je i prikazano na slici 6.

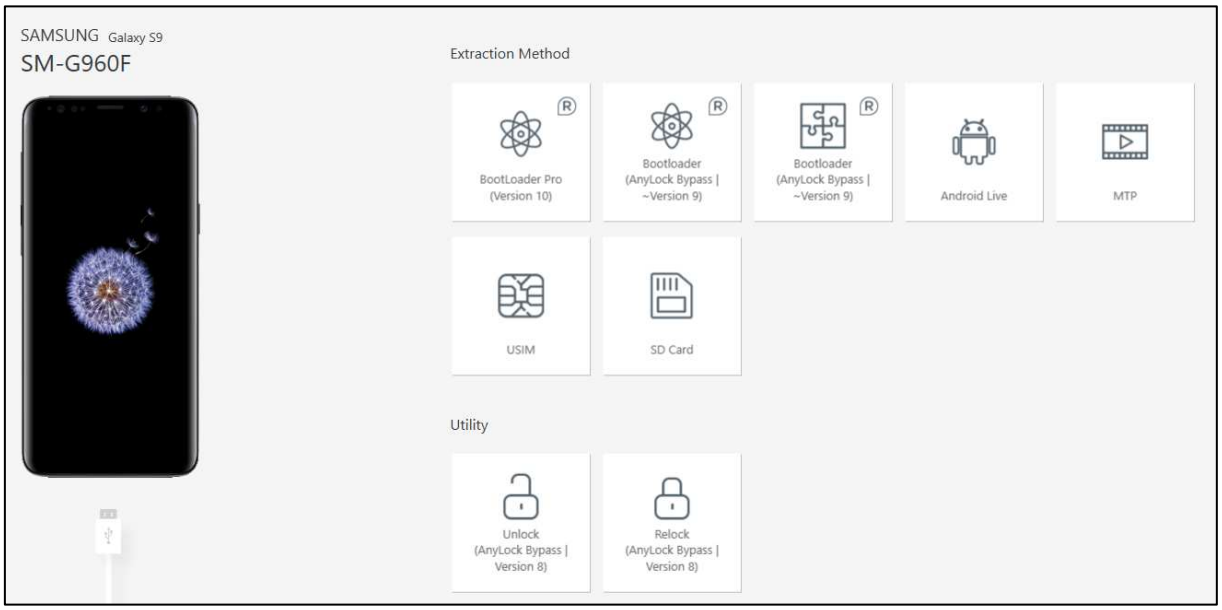


Slika 6. Odabir modela pametnog telefona

Izvor: Autor (osobni primjer)

Odabir željene metode ekstrakcije

Ovisno o potrebama i zahtjevima istrage, istražitelj odabire određenu vrstu ekstrakcije što je u ovom slučaju logička ekstrakcija. Na slici 7 prikazano je sučelje forenzičkog alata na kojemu su vidljive moguće vrste ekstrakcije za odabrani uređaj.

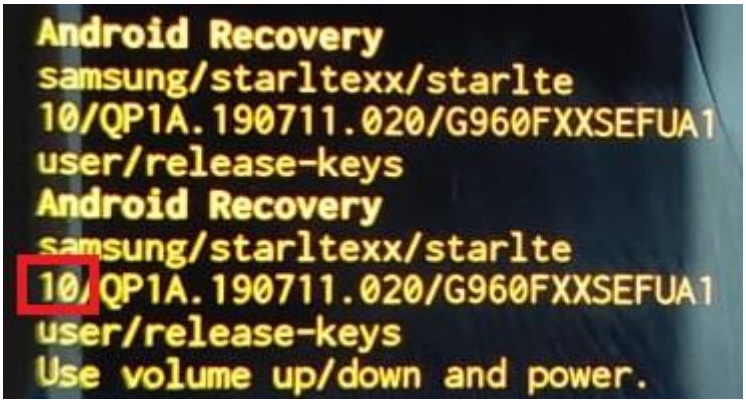


Slika 7. Ponuđene vrste ekstrakcije

Izvor: Autor (osobni primjer)

Identifikacija verzije androida

Nakon što je odabrana metoda ekstrakcije, MD – NEXT zahtijeva odabir verzije Androida što je potrebno izvesti pomoću kombinacije tipki. Kako bi uređaj ušao u *Android Recovery* mod potrebno je istovremeno pritisnuti i držati tipke *Volume Up + Home + Bixby*, nakon toga uređaj ulazi u *Android Recovery* mod što je prikazano na slici 8. U crvenom pravokutniku označen je broj Android verzije što je bitno za daljnje postupke u procesu ekstrakcije podataka.



Slika 8. *Android Recovery* mod

Izvor: Autor (osobni primjer)

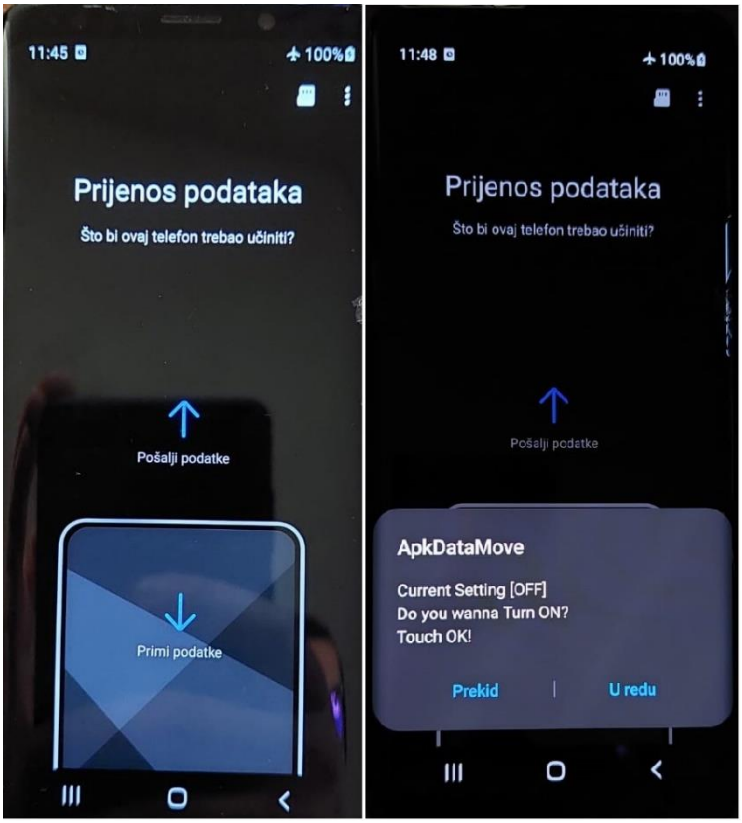
Provjera postavki uređaja

Za uspješno provedenu ekstrakciju podataka s uređaja Samsung Galaxy S9 potrebno je izvršiti provjeru određenih naprednih postavki. Ukoliko pod postavkama uređaja nije moguće odabrati kategoriju *Opcije razvoja,* tada je potrebno pod kategorijom *O telefonu* 7 puta kliknuti na *Build number* kako bi se omogućila i prikazala kategorija *Opcije razvoja.* U toj kategoriji potrebno je aktivirati opciju *Otklanjanje poteškoća putem USB-a* i kao zadanu USB konfiguraciju postaviti *MTP.*

Nakon toga u postavkama pod kategorijom *Aplikacije* potrebno je prisilno zaustaviti sve aplikacije koje se izvode na početnom zaslonu i deaktivirati aplikacije koje imaju mogućnosti skočnih obavijesti. Nadalje, pod kategorijom *Zaslon* potrebno je isključiti filter plavog svjetla.

Prijenos podataka

Na slici 9 prikazano je sučelje uređaja na kojemu je potrebno odabrati željenu radnju koju bi uređaj trebao izvršiti, u ovom slučaju to je radnja *Pošalji podatke* koja omogućava slanje podataka na računalo, tj. omogućava logičku ekstrakciju. Na slici 9 prikazan je status *ApkDataMove* aplikacije koji mora biti *Current Setting[OFF].*



Slika 9. Slika zaslona uređaja tijekom odabira postavki za ekstrakciju podataka

Izvor: Autor (osobni primjer)

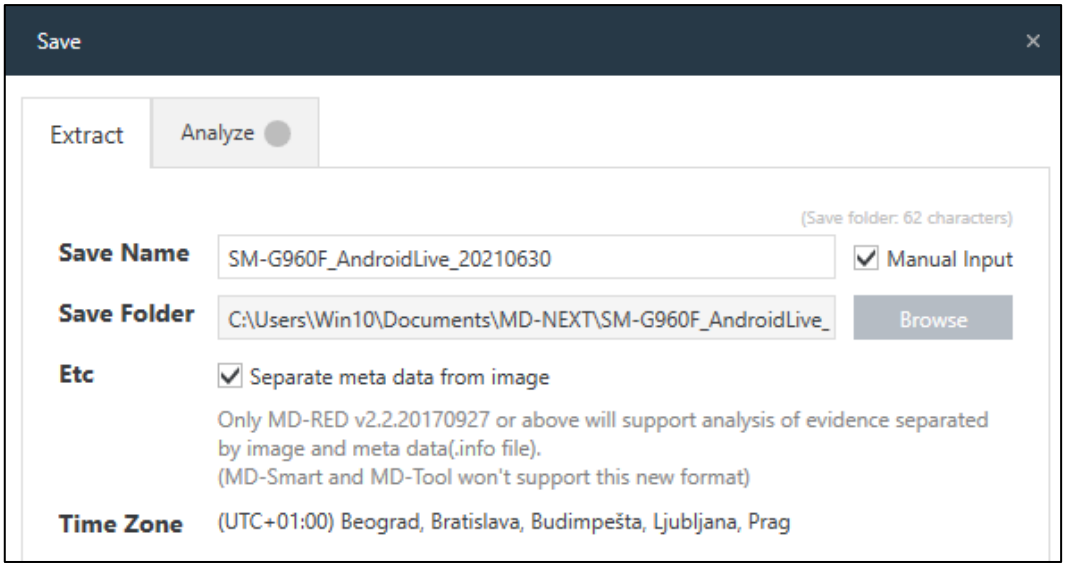
Odabir potpune ili selektivne ekstrakcije

Kako je pametni telefon uređaj koji prikuplja veliku količinu raznovrsnih podataka, u slučajevima kada se radi o sudskom procesu često se zahtijeva ekstrakcija samo određenih

aplikacija ili samo određenih vrste podataka za što se koristi selektivna ekstrakcija. U slučaju koji je opisan u ovom diplomskom radu izvršiti će se potpuna ekstrakcija.

Postavljanje parametara za pohranu forenzičke slike

Parametri prikazani na slici 10 prikazuju odabir datotečne putanje koja predstavlja mjesto pohrane forenzičke slike na istražiteljevom računalu, ime forenzičke slike te odabir vremenske zone.



Slika 10. Parametri pohrane forenzičke slike

Izvor: Autor (osobni primjer)

Davanje dopuštenja aplikaciji MdLiveContentReader

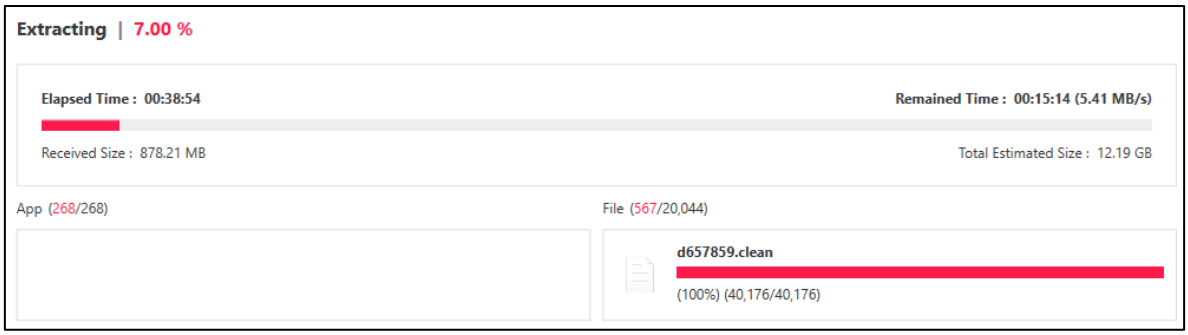
Nakon postavljanja parametara za pohranu forenzičke slike, MD – NEXT forenzički alat zahtijeva od istražitelja da pomoću korisničkog sučelja uređaja Galaxy S9 omogući određena dopuštenja aplikaciji MdLiveContentReader. Dopuštenja se odnose na kontakte, telefonske pozive, kalendar, zapise telefonskih poziva, fotografije, medije, datoteke i SMS poruke.

Izrada pune sigurnosne kopije

MD – NEXT generira zahtjeva za izradom potpune sigurnosne kopije, nakon što se izradi sigurnosna kopija pokreće se proces ekstrakcije podataka.

Ekstrakcija podataka

Na slici 11 prikazano je sučelje računala na kojemu je vidljiv proces ekstrakcije podataka, u ekstrakciji podataka obrađuje se 268 aplikacija i 20 044 datoteke, koje ukupno zauzimaju 12,19 GB (gigabajta) memorije na uređaju koji je predmet istrage.



Slika 11. Izvršavanje procesa ekstrakcije podataka

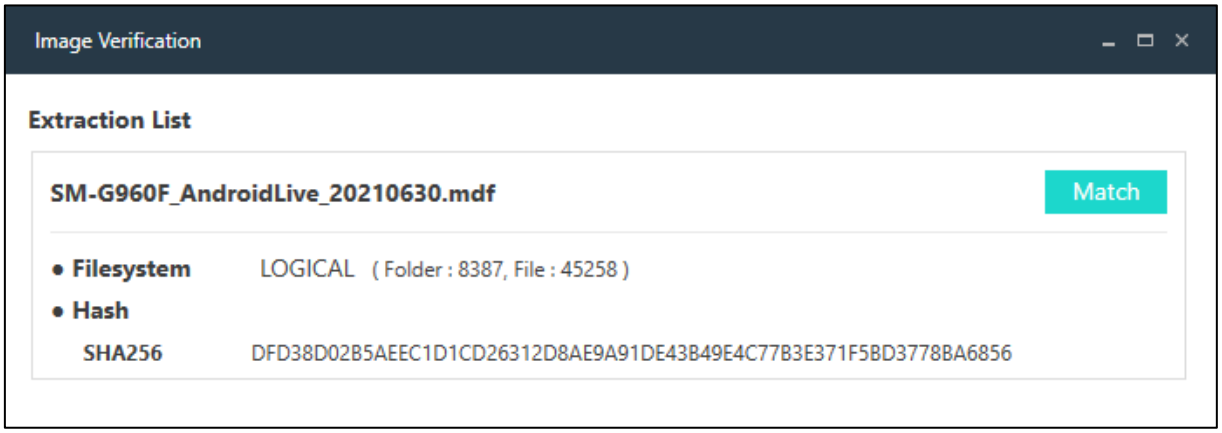
Izvor: Autor (osobni primjer)

Potvrđivanje vraćanja degradiranih aplikacija u izvorno stanje

Kako bi forenzički alat uspješno izvršio ekstrakciju podataka, omogućen mu je proces manipulacije nad aplikacijama koje su bitne za istragu. Nakon toga aplikacije je potrebno vratiti u izvorno stanje što je izvršeno pomoću *Downgrade App Restore* opcijom u samom MD – NEXT alatu. Aplikacije koje su vraćene u izvorno stanje su sljedeće: Facebook Messenger, Google Drive, Instagram, Skype, Viber, WhatsApp, Telegram, Signal Private Messenger.

Verifikacija forenzičke slike

Na slici 12 prikazan je završni izvještaj ekstrakcije koji prikazuje ime forenzičke slike, metodu ekstrakcije, broj prikupljenih direktorija, broj prikupljenih datoteka i *hash* vrijednost u SHA256 formatu.

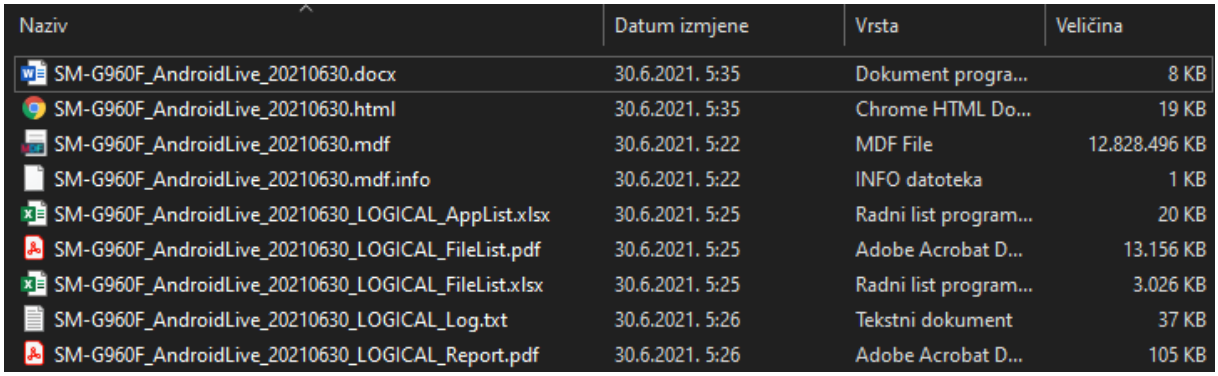


Slika 12. Verifikacija forenzičke slike

Izvor: Autor (osobni primjer)

Nakon uspješne provedbe ekstrakcijske metode, MD – NEXT istražitelju nudi automatsku analizu prikupljenih podataka u forenzičkom softverskom alatu MD – RED. U ovom slučaju to nije prakticirano, nakon završetka logičke ekstrakcije pokrenuta je fizička ekstrakcija koja je opisana u nastavku.

Datoteke koje su generirane nakon završetka procesa logičke ekstrakcije prikazane su na slici 13, a podrazumijevaju izvještaj o ekstrakciji u nekoliko formata, popis aplikacija prikupljenih logičkom ekstrakcijom, popis datoteka prikupljenih logičkom ekstrakcijom i *log* zapis.



Naziv	Datum izmjene	Vrsta	Veličina
SM-G960F_AndroidLive_20210630.docx	30.6.2021. 5:35	Dokument progra...	8 KB
SM-G960F_AndroidLive_20210630.html	30.6.2021. 5:35	Chrome HTML Do...	19 KB
SM-G960F_AndroidLive_20210630.mdf	30.6.2021. 5:22	MDF File	12.828.496 KB
SM-G960F_AndroidLive_20210630.mdf.info	30.6.2021. 5:22	INFO datoteka	1 KB
SM-G960F_AndroidLive_20210630_LOGICAL_AppList.xlsx	30.6.2021. 5:25	Radni list program...	20 KB
SM-G960F_AndroidLive_20210630_LOGICAL_FileList.pdf	30.6.2021. 5:25	Adobe Acrobat D...	13.156 KB
SM-G960F_AndroidLive_20210630_LOGICAL_FileList.xlsx	30.6.2021. 5:25	Radni list program...	3.026 KB
SM-G960F_AndroidLive_20210630_LOGICAL_Log.txt	30.6.2021. 5:26	Tekstni dokument	37 KB
SM-G960F_AndroidLive_20210630_LOGICAL_Report.pdf	30.6.2021. 5:26	Adobe Acrobat D...	105 KB

Slika 13. Generirane datoteke nakon završene logičke ekstrakcije

Izvor: Autor (osobni primjer)

5.3.3 Postupak fizičke ekstrakcije podataka

Kod fizičke ekstrakcije podataka omogućeno je prikupljanje podataka koji nisu dostupni korištenjem logičke ekstrakcije, samim time fizička ekstrakcija prikuplja veću količinu podataka što istražitelju daje detaljniji i precizniji uvid u dokaze koji mogu biti korisni u sudskom procesu. U forenzičkom alatu MD – NEXT fizička ekstrakcija navedena je pod nazivom Bootloader Pro koji može biti konfiguriran za Android verziju 9 i Android verziju 10, u ovom slučaju korišten je Bootloader Pro za Adroid verziju 10.

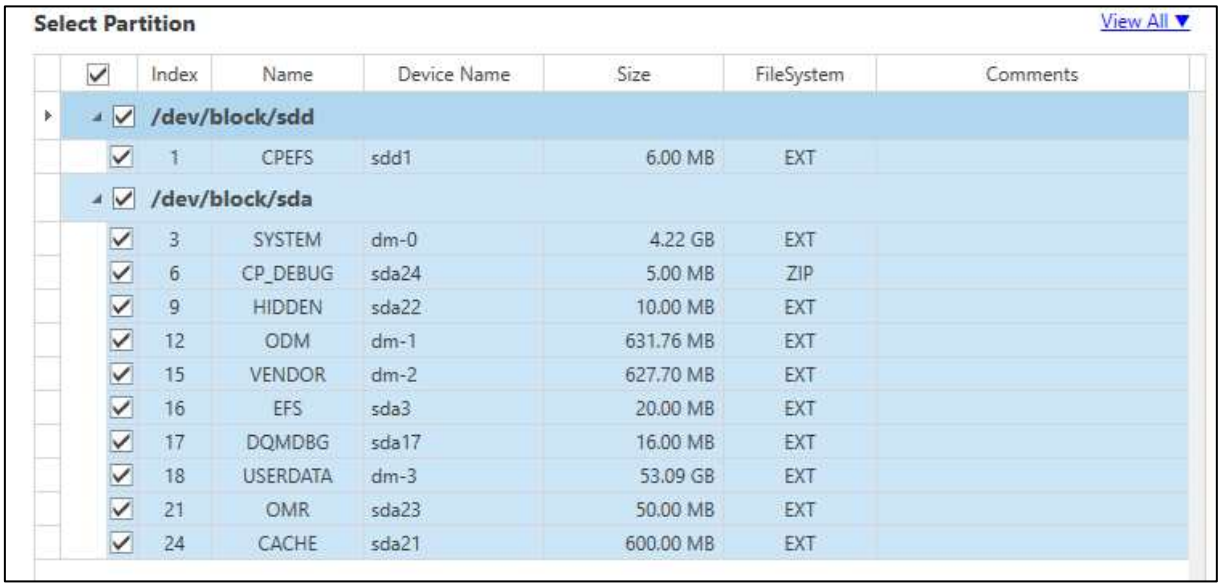
Postupci koji opisuju povezivanje uređaja, automatsko prepoznavanje uređaja, odabir željene metode ekstrakcije, identifikacija verzije androida i provjera postavki uređaja identični su kao i kod provođenja procesa logičke ekstrakcije te se iz tog razloga neće ponovno opisivati.

Pokretanje *Download mode* procesa

Kako bi MD – NEXT uspješno prikupio sve podatke iz uređaja potrebno mu je dati ovlasti koje imaju mogućnost manipulacije temeljnih pokretačkih programa kako bi se omogućilo čitanje memorije koja je prividno izbrisana ali nije prepisana. Iz tog razloga istražitelj mora pokrenuti *Download mode* proces na način da nakon što je uređaj ugašen i nakon što je prekinuta USB veza između uređaja i računala, istovremeno pritisne i drži pritisnutim tipke *Volume Download + Bixby + Power.* Kada uređaj pokrene *Download mode* istražitelj mora ponovno povezati uređaj i računalo putem USB kabela. Nakon što istražitelj izvrši pritiskanje navedenih tipki uređaj pokrene upozorenje o pokušaju pokretanja *Download mode* procesa, pritiskom tipke *Volume Up* uređaj nastavlja s pokretanjem *Download mode* procesa.

Odabir particija

Istražitelj ima mogućnost odabira datotečnih particija kako bi preciznije usmjerio istragu ukoliko ima potrebe za time. Na slici 14 prikazano je programsko sučelje putem kojeg istražitelj ima uvid u nazive, veličinu i vrstu pojedine particije te izvršava odabir željenih particija.



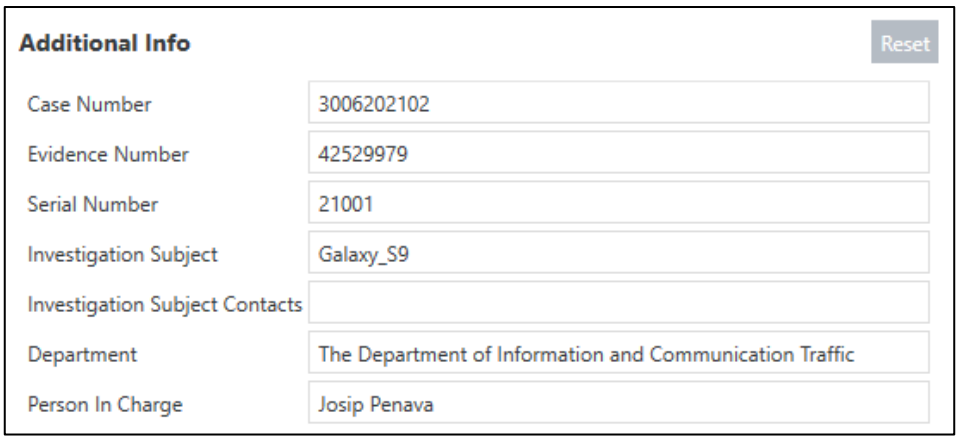
Index	Name	Device Name	Size	FileSystem	Comments
	/dev/block/sdd				
1	CPEFS	sdd1	6.00 MB	EXT	
	/dev/block/sda				
3	SYSTEM	dm-0	4.22 GB	EXT	
6	CP_DEBUG	sda24	5.00 MB	ZIP	
9	HIDDEN	sda22	10.00 MB	EXT	
12	ODM	dm-1	631.76 MB	EXT	
15	VENDOR	dm-2	627.70 MB	EXT	
16	EFS	sda3	20.00 MB	EXT	
17	DQMDBG	sda17	16.00 MB	EXT	
18	USERDATA	dm-3	53.09 GB	EXT	
21	OMR	sda23	50.00 MB	EXT	
24	CACHE	sda21	600.00 MB	EXT	

Slika 14. Odabir datotečnih particija

Izvor: Autor (osobni primjer)

Postavljanje parametara za pohranu forenzičke slike

Kao i kod logičke ekstrakcije podataka, i u ovom slučaju potrebno je odrediti ime pod kojim će se pohraniti forenzička slika, datotečnu putanju na računalu gdje će slika biti pohranjena i odabir zasebnog generiranja meta podataka. Uz to, na slici 15 prikazani su podaci o slučaju koji podrazumijevaju broj slučaja, broj dokaza, serijski broj, subjekt istrage, istraživački odjel i ime istražitelja.



Slika 15. Informativni podaci o slučaju

Izvor: Autor (osobni primjer)

Ekstrakcija podataka

Izvršava se segmentirano tj. svaka particija se ekstrahira zasebno, te se na kraju ekstrakcije generira izvješće koje sadrži relevantne podatke za istragu. U ovom slučaju kada se izvršava fizička ekstrakcija podataka, trajanje ekstrakcije trajalo je 52 minute i 6 sekundi dok je proces logičke ekstrakcije trajao 59 minuta i 20 sekundi.

U tablici 7 navedene su sve particije po redoslijedu izvršavanja, u tablici je naveden naziv particije, veličina particije i količina prikupljenih podataka, uz to izvješće o ekstrakciji sadrži još dodatno i SHA256 vrijednosti koje nisu navedene u tablici.

Tablica 7. Popis particija i pripadajuće vrijednosti

Naziv particije	Veličina particije (bajta)	Količina prikupljenih podataka (bajta)
CPEFS	6,291,456	6,291,456
SYSTEM	4,530,393,088	4,530,393,088
CP_DEBUG	5,242,880	5,242,880
HIDDEN	10,485,760	10,485,760
ODM	662,446,080	662,446,080
VENDOR	658,186,240	658,186,240
EFS	20,971,520	20,971,520
DQMDBG	16,777,216	16,777,216
USERDATA	57,004,769,280	57,004,769,280
OMR	52,428,800	52,428,800
CACHE	629,145,600	629,145,600
SYSTEM_BACKUP	36,864	36,864
KNOXDATA	792,358,912	792,358,912

Izvor: Autor (osobni primjer)

Potrebno je napomenuti kako je iz tablice 9 moguće uočiti da su sve particije u potpunosti ekstrahirane što je potvrđeno usporedbom veličine particije i količine prikupljenih podataka gdje je uočeno kako nema razlike između te dvije vrijednosti.

Verifikacija forenzičke slike

Nakon završetka ekstrakcije i generiranja izvješća moguće je verificirati forenzičke slike na način da se usporede *hash* vrijednosti koje su zapisane u SHA256 formatu. Forenzičke slike MD – NEXT forenzičkog alata imaju ekstenziju *.mdf* koja je kompatibilna s MD – RED forenzičkim alatom za analizu prikupljenih podataka.

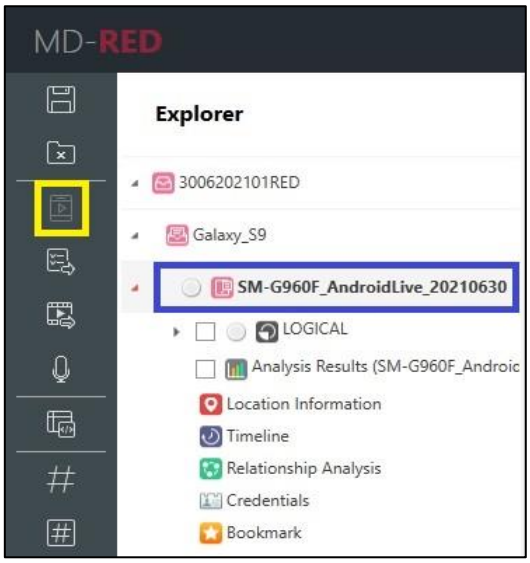
6. Analiza ekstrahiranih podataka mobilnih aplikacija

U ovom diplomskom radu za analizu prikupljenih podataka korišten je forenzički alat MD – RED tvrtke Hancom. Jedna od bitnih funkcionalnosti ovog alata je segmentacija podataka na osnovu aplikacija za trenutačnu razmjenu poruka. Takva funkcionalnost istražitelju omogućava lakšu selekciju podataka što utječe na očuvanje integriteta i cjelovitosti dokaza koji su ponekad od ključnog značaja za slučaj. Tijekom provedbe forenzičke analize prikupljenih podataka aplikacije koje su bile u središtu istrage su WhatsApp, FacebookMessenger i Viber, uz njih MD – RED prepoznao je i neke druge poput Instagrama, Signala, Telegrama i nekih drugih manje popularnih aplikacija za trenutačnu razmjenu poruka.

S obzirom da su tijekom ekstrakcije podataka korištene dvije metode, logička ekstrakcija i fizička ekstrakcija, analiza podataka biti će segmentirana u dva osnovna dijela. Prvi dio ovoga poglavlja odnositi će se na analizu forenzičke slike koja je rezultat logičke ekstrakcije, dok će se u drugom dijelu analizirati forenzička slika koja je rezultat fizičke ekstrakcije uređaja.

6.1 Analiza podataka dobivenih logičkom ekstrakcijom

Nakon što je uspješno izvršena logička ekstrakcija uređaja i generirano izvješće slijedi analiza forenzičke slike pod nazivom *SM-G960F_AndroidLive_20210630.mdf.* Na samom početku MD – RED od istražitelja zahtjeva imenovanje grupe i dodavanje forenzičke slike. Nakon što je odabrana prethodno navedena forenzička slika započinje proces dodavanja slike u MD – RED okruženje. Istražitelj zatim odabire dodanu sliku na način da označi forenzičku sliku u *Explorer* bočnom prozoru (slika 16, plavi pravokutnik) i potom pokreće analizu što je i prikazano na slici 16 (žuti pravokutnik).



Slika 16. MD-RED *explorer* bočni prozor

Izvor: Autor (osobni primjer)

Kao što je prije već spomenuto, MD – RED segmentira analizirane podatke ovisno o aplikaciji koja je generirala podatke tijekom korištenja pametnog telefona. U nastavku teksta navedeni su rezultati analize za pojedine aplikacije koje su od interesa u ovoj istrazi.

6.1.1 WhatsApp

Kako je WhatsApp i na globalnoj razini najkorištenija aplikacija za trenutačnu razmjenu poruka, što je i opisano u poglavlju „2. Korištenje pametnih telefona i aplikacije za trenutačnu razmjenu poruka“, u ovom slučaju WhatsApp aplikacija uvelike prednjači s količinom prikupljenih podataka. Prilikom logičke ekstrakcije uređaja prikupljeno je 177,223 zapisa koji se odnose na WhatsApp aplikaciju, od kojih je 1,233 izbrisanih zapisa. U nastavku su opisane kategorije podataka koje je automatski generirao MD – RED nakon uspješne analize forenzičke slike.

Korisnički račun

Sadrži 4 retka koji su opisani sljedećim parametrima: aplikacija, status, domena, artikl i sadržaj. Jedan od redaka odnosi se na postojeći korisnički račun koji je korišten na uređaju dok se ostala 3 odnose na korisničke račune korištene tijekom prijave putem web preglednika. Korisnički računi korišteni za prijavu putem web preglednika sadrže informacije o korištenom operativnom sustavu računala na kojemu je izvršena prijava (Windows), vrstu web preglednika (Chrome, Firefox) te datum i vrijeme prijave.

Kontakti

Sadrži 1,423 kontakata od kojih su neki kontakti koji su pohranjeni na uređaju dok su ostali kontakti koji su u istim grupnim razgovorima kao i korisnik uređaja koji je predmet istrage. Tablica kontakti sadrži informacije kao što je broj mobilnog telefona, ime prikazano u aplikaciji, ime pod kojim je kontakt pohranjen, sadrži li kontakt adresu elektroničke pošte, datum kreiranja kontakta od strane korisnika uređaja, postojanje slike profila i vidljivog statusa kontakta.

Povijest poziva

Sastoji se od glasovnih i video poziva, sadrži 2,005 redaka od kojih je moguće segmentirati dolazne i odlazne pozive. Tablica sadrži informacije poput statusa poziva (aktivno ili izbrisano), vrste poziva, ime kontakta, broj mobilnog telefona, vrijeme i datum uspostave poziva i trajanje poziva.

Poruke

Tablica koja sadrži 172,862 retka, prikazuje informacije kao što su vrsta poruke (dolazna ili odlazna), vrijeme i datum nastanka poruke, sadržaj poruke, prilozi ukoliko ih ima (slika, audio zapis, datoteka, web poveznica, itd.), broj mobilnog telefona primatelja i pošiljatelja i status poruke (šalje se, poslano, primljeno, pročitano).

Povijest statusa

Opisuje statuse korisnika koji su podijelili određeni multimedijski zapis sa svim svojim kontaktima. Tablica sadrži dva zapisa koji sadrže podatke o vrsti poruke, vremenu i datumu stvaranja, sadržaju i datotečnoj putanji.

Chat sobe

Tablica sadrži 926 zapisa koji se odnose na sve individualne i grupne razgovore u kojima je korisnik sudjelovao. Sadržaj ove tablice pogodan je za stvaranje grafikona međusobnih veza između korisnika i drugih sudionika koji bi mogli biti od interesa za istragu.

Povijest karte

Sadrži jedan zapis koji ukazuje na geografsku lokaciju koju je korisnik primio u poruci kao prilog. Geografska lokacija definirana je zemljopisnom visinom i širinom.

6.1.2 Facebook Messenger

Posebnost ove aplikacije je ta što uz interakciju s korisnikom istovremeno komunicira s aplikacijom Facebook koja joj šalje informativne poruka kako bi se potaknulo korisnika na korištenje iste. Tijekom logičke ekstrakcije uređaja prikupljeno je 1,367 zapisa od kojih je 150 izbrisano. U nastavku su navedene neke od kategorija podataka koje mogu biti zanimljive i korisne tijekom istrage. Potrebno je napomenuti kako se kategorije podataka puno ne razlikuju od kategorija WhatsApp ili Viber aplikacije.

Korisnički račun

Sadrži podatke o korisnikovom računu koji je povezan s Facebook aplikacijom, a prikazuje podatke kao što su: ime i prezime korisnika, ID korisnika, ID uređaja, vrijeme i datum kreiranja ID-a uređaja, adresu e-pošte, spol, država i slika profila. Ovi podaci mogu biti od velike koristi tijekom istrage iz razloga što nude informacije koje nisu učestale za aplikacije ovog tipa.

Kontakti

Ukupno njih 771 koji su generirani u kontekstu individualnih ili grupnih razgovora. Sadrže informacije o statusu Facebook prijatelja, ime i nadimak Facebook prijatelja, ID-u i slici profila.

Povijest poziva

Tablica sadrži samo dva zapisa koji prikazuju informacije o vrsti poziva (dolazni ili odlazni), imenu i prezimenu korisnika koji je dio komunikacijskog procesa, datumu i vremenu uspostave poziva i vremenu trajanja poziva.

Poruke

Sadrži 364 zapisa koji uz ime i prezime Facebook prijatelja prikazuju informacije o sadržaju poruke, datumu i vremenu slanja ili primanja poruke, identifikatoru svake poruke te identifikatoru *chat* sobe.

Chat sobe

Tablica s ukupno 210 zapisa koji uz ime Facebook prijatelja ili generirane grupe korisnika sadrži podatke o datumu i vremenu posljednje poruke te ukoliko je riječ o grupnom razgovoru prikazuje sve korisnike koji su dio istog.

Log zapisi

Mali broj od 16 zapisa koji prikazuju vrstu obavijesti, datum i vrijeme primanja iste. Obavijesti su najčešće nekog reklamnog sadržaja ili preporuka za slanje zahtjeva za prijateljstvo osobama za koje Facebook odluči da bi mogli imati interesa.

Aplikacije

Jedan zapis koji navodi ime aplikacije, status, ime paketa iz kojega je aplikacija instalirana, broj verzije, vrijeme i datum prve instalacije, posljednje nadogradnje i posljednjeg korištenja.

6.2 Analiza podataka dobivenih fizičkom ekstrakcijom

Kako je fizička ekstrakcija puno detaljnija i prikuplja veću količinu podataka, u ovom odlomku opisati će se neke pojedinosti koje nisu bile vidljive tijekom analize logičke ekstrakcije. Iz razloga što je u prethodnom naslovu detaljnije opisana pojedina aplikacija, u ovome dijelu diplomskog rada pozornost je na podacima koji su djelomični iz razloga što su oporavljeni upotrebom fizičke ekstrakcije. Osim toga, opisati će se i načini filtriranja skupa podataka kako bi se segmentirale željene informacije vezane za podatke aplikacija ta trenutačnu razmjenu poruka.

6.2.1 WhatsApp

Jedna od najbitnijih i najčešće korištenih mogućnosti forenzičkih softverskih alata je filtriranje i sortiranje podataka. Ovim postupcima istražitelj može uvelike smanjiti obujam podataka što mu olakšava analizu istih. Manipulacijom manjeg broja podataka dokazi mogu biti vjerodostojniji i cjelovitiji što su jedni od temeljnih kriterija za uspješnu provedbu forenzičke analize.

Na slici 17 prikazana je tablica povijesti poziva WhatsApp aplikacije na kojoj je primijenjen filter u tekstualnom obliku koji je od 2,005 zapisa izdvojio njih 474. Osim filtriranja podataka primijenjeno je i sortiranje istih s obzirom na duljinu trajanja poziva i to u silaznom poretku.

U forenzičkom alatu MD – RED moguće je filtrirati podatke s obzirom na njihovu vrstu, na taj način je generiran broj od 615 primljenih audio poziva, 310 upućenih audio poziva, 454 primljenih video poziva i 331 upućeni video poziv.

Filtriranjem statusa poziva generirana je brojka od 295 izbrisanih poziva koji su u većini primjera povezani s izbrisanim kontaktima.

Find

Check Count = 0 Total Count = 2,005 **Display Count = 474**

Drag a column header here to group by that column

Type	Name	Contacts	Time	Duration	Chat Room	Group
Receive Video Call	Marijičica	+385919230325	Time : 04/08/2021 22:06:19	02:47:16	385919230325@s.whatsapp.net	
Receive Video Call	Marijičica	+385919230325	Time : 12/13/2020 23:44:35	02:02:49	385919230325@s.whatsapp.net	
Send Video Call	Marijičica	+385919230325	Time : 12/16/2020 00:24:08	01:41:21	385919230325@s.whatsapp.net	
Send Video Call	Marijičica	+385919230325	Time : 12/20/2020 23:23:31	01:38:27	385919230325@s.whatsapp.net	
Send Video Call	Marijičica	+385919230325	Time : 12/19/2020 14:38:15	01:02:03	385919230325@s.whatsapp.net	
Send Video Call	Marijičica	+385919230325	Time : 03/19/2021 01:39:11	01:01:45	385919230325@s.whatsapp.net	
Send Video Call	Marijičica	+385919230325	Time : 02/16/2021 00:55:41	00:56:16	385919230325@s.whatsapp.net	

Slika 17. Filtriranje i sortiranje podataka

Izvor: Autor (osobni primjer)

Podatke koje sadrži kontakt lista WhatsApp aplikacije mogu biti od važnosti za istragu iz razloga što uz osnovne informacije o korisniku prikazuje sljedeće:

- vrijeme nastanka statusa korisničkog profila,
- vrstu uređaja s kojeg se vrši komunikacija,
- oznaka uređaja s kojeg se vrši komunikacija,
- vrijeme nastanka slike profila,
- vrijeme postavljanja slike profila,
- prezime korisnika,
- nadimak korisnika,
- ime poduzeća,
- oznaku poslovnog profila.

Neki korisnici WhatsApp aplikaciju koriste kao platformu za provedbu vlastitog poslovanja što samoj aplikaciji daje na vrijednosti, a samim time i podacima koje ona generira i pohranjuje. Na slici 18 tablično je prikazan poslovni profil koji sadrži podatke poput adrese e-pošte, adrese poduzeća i naziv poduzeća.

State	Name	Email	Status	Others
Active	Tomislav		Hey there!	
Active	Friend name by friend : Tomislav		Tomislav	
Active	Friend name by friend : Tomislav		.	
Active	Friend name by friend : Tomislav	tkstarina@gmail.com	Some people never live, but crazy ones never die	Address : Šulinec 34 Sveti Ivan Zelina Description : ABC rent

Slika 18. Poslovni podaci WhatsApp kontakta

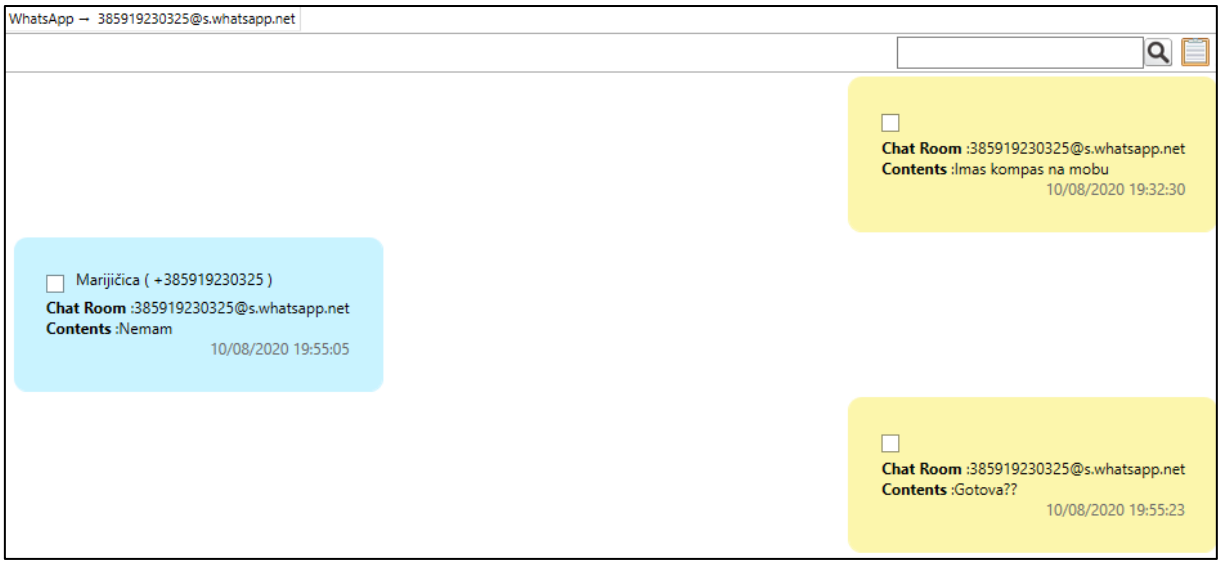
Izvor: Autor(osobni primjer)

Kao što je prije spomenuto kako MD – RED nudi mogućnost filtriranja podataka s obzirom na vrstu i status, na slici 19 prikazan je padajući izbornik koji prikazuje vrste WhatsApp poruka koje mogu biti individualno ili grupno filtrirane.

Slika 19. Opcije filtriranja poruka po vrsti

Izvor: Autor (osobni primjer)

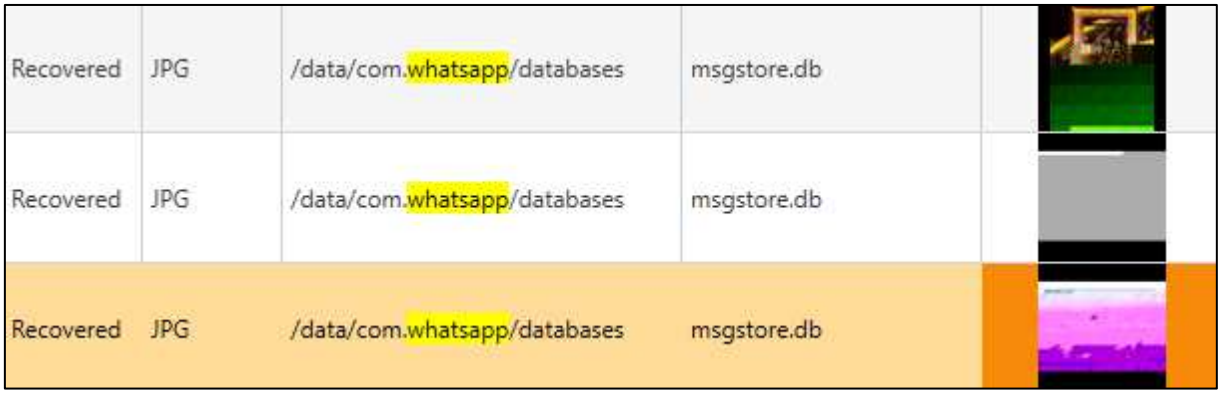
MD – RED je jedan od suvremenijih forenzičkih softverskih alata koji nudi mogućnost vizualizacije aplikativnog sučelja čime se istražitelju olakšava analiziranje podataka ali i predstavljanje dokaza na sudu što je u nekim sudskim procesima od krucijalne važnosti. Na slici 20 prikazana je vizualizacija korisničkog sučelja za određeni filtrirani kontakt. Na ovaj način istražitelj lakše manipulira kroz vremenski slijed poruka čime mu se smanjuje vrijeme trajanja procesa forenzičke analize.



Slika 20. Vizualizacija WhatsApp razgovora

Izvor: Autor (osobni primjer)

Pošto fizička ekstrakcija ima mogućnost prikupljanja podataka koji su prepisani u memorijskim klasterima, na slici 21 prikazane su fotografije čija je struktura narušena iz razloga što je na njihovo mjesto u memorijskim klasterima zapisana nova datoteka. Dio slike koji je vidljiv iščitava se iz *space slack*-ova koji su ostali netaknuti.



Slika 21. Djelomično oporavljene fotografije

Izvor: Autor (osobni primjer)

U sljedećem odlomku osvrt će biti na aplikaciji Facebook Messenger koja ima određenih sličnosti aplikaciji WhatsApp, pa se zbog toga neki podaci neće opisivati. Potencijalno je navesti podatke o kontaktima koji sadrže informacije od interesa za istragu.

6.2.2 Facebook Messenger

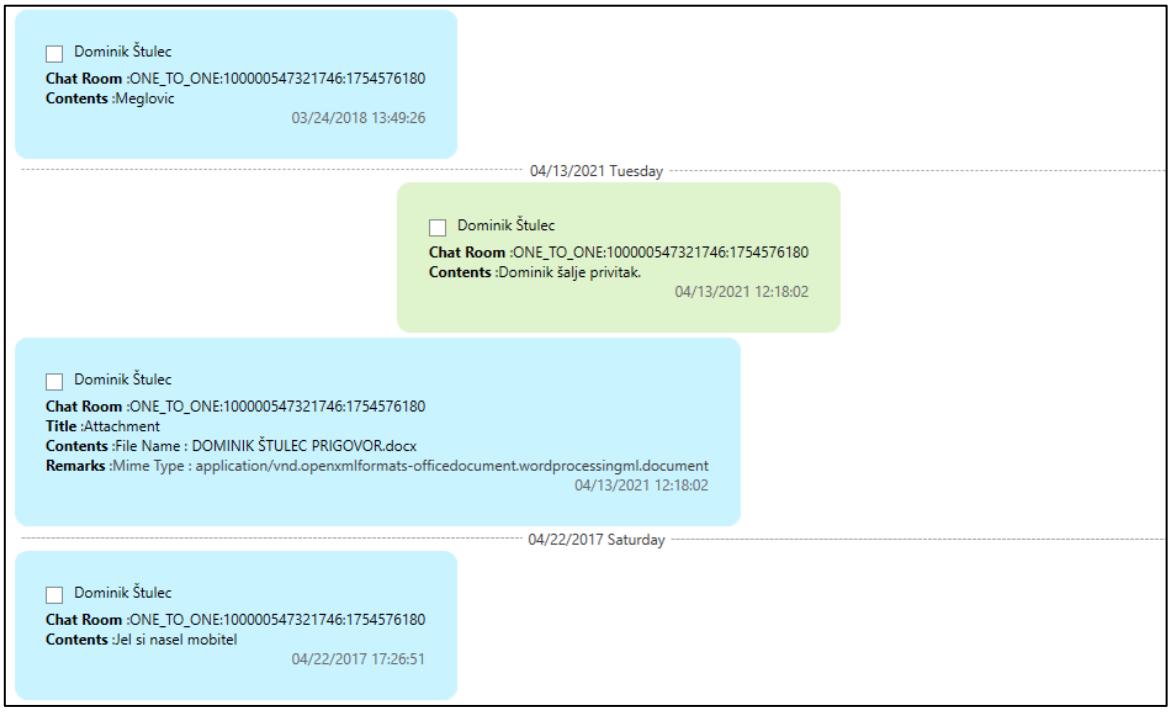
Analizom baze podataka Facebook Messenger aplikacije uočeni su zanimljivi podaci koji mogu imati ključnu ulogu u povezivanju uređaja s određenim kriminalnim radnjama, ukoliko je to navedeno u sudskom nalogu.

Kontakt lista

Osim osnovnih podataka poput imena, prezimena, korisničkog imena i slike profila, kontakt lista sadrži podatke o tome koristi li Facebook korisnik aplikaciju Facebook Messenger, koju vrstu profila korisnik koristi (privatni ili poslovni). Osim toga moguće je iščitati je li korisnik blokiran ili jesu li mu blokirane poruke ukoliko su zlonamjernog sadržaja. Nadalje, kontakt lista sadrži informacije radi li se o Facebook prijatelju ili ne, moguće je odrediti datum i vrijeme posljednjeg pregledavanja razgovora od strane drugih korisnika te radi li se o automatskoj poruci ili je poruka natipkana od strane korisnika.

Poruke

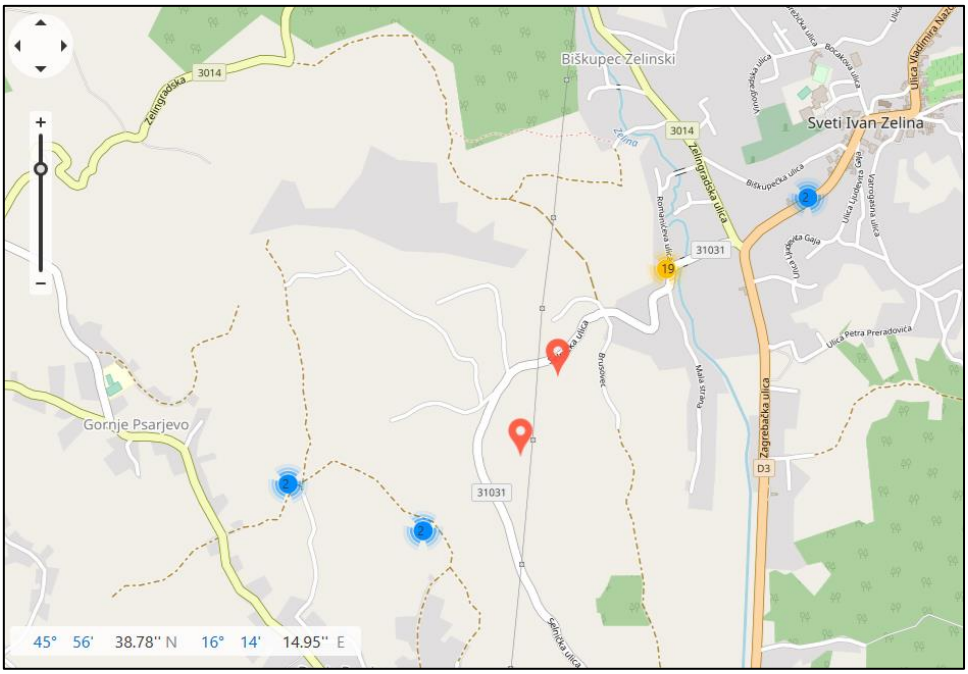
Analizom poruka prikupljenih fizičkom ekstrakcijom primijećeno je kako su poruke koje su prikupljene generirane 2015. godine, dok je uređaj Galaxy S9 nije niti bio proizveden. Uređaj je prvi put korišten 2019. godine te se je koristio do 2021. godine. Ovaj podatak pokazuje koliko je analiza aplikacija za trenutačnu razmjenu poruka bitna iz razloga što sama aplikacija na svojim udaljenim pohranama čuva poruke koje mogu biti od velikog interesa tijekom istrage. Na slici 22 prikazana je vizualizacija poruka koja realnije prikazuje tijek razgovora što istražitelju daje mogućnost brže analize prikupljenih podataka.



Slika 22.Vizualizacija Facebook Messenger poruka

Izvor: Autor (osobni primjer)

Jedna od popularnih karakteristika MD – RED alata je kartografski prikaz lokacija koje su prikupljene tijekom ekstrakcije a odnose se na podatke generirane u Facebook Messenger i WhatsApp aplikacijama.



Slika 23. Kartografski prikaz lokacija

Izvor: Autor (osobni primjer)

Na slici 23 prikazana je karta područja oko grada Sveti Ivan Zelina na kojoj je moguće vidjeti da su lokacije povezane s frekventnim adresama na kojima je uređaj uspostavljao Internet vezu te slao i primao poruke.

6.3 Usporedba količine dobiveni podataka logičkom i fizičkom ekstrakcijom

Kao što je u prijašnjim odlomcima opisano, fizička ekstrakcija prikuplja veću količinu podataka iz razloga što se temelji na pokretanju temeljnih kodova. Djelovanjem na jezgru Android sustava moguće je prikupiti podatke koji nisu vidljivi putem korisničkog sučelja što je za forenzičku analizu od velike važnosti. U tablici 8 navedene su kategorije podataka te njihova količina ovisno o korištenoj metodi ekstrakcije.

Tablica 8. Usporedba količine prikupljenih podataka

Vrsta podatka	Logička ekstrakcija	Fizička ekstrakcija
Korisnički račun	23	335
Informacije	9	55
Kontakti	3,550	6,543
Grupe kontakata	68	35

Povijest poziva	4,035	4,512
Poruke	188,232	198,734
Povijest društvenih medija	2	473
Chat sobe	1,602	2,113
Raspored	233	231
Povijest preglednika	2	2,836
Log zapis *cloud* usluge	2,587	16,532
Log zapis	50	39,209
Povijest karata	1	12
Aplikacije	849	2,427
Multimedijski zapisi	59,572	161,629

Izvor: Autor (osobni primjer)

Tablicom 8 dokazana je efikasnost fizičke ekstrakcije podataka koja je u većini slučajeva prikupila nekoliko puta veću količinu podataka iste vrste. Potrebno je napomenuti kako se logička ekstrakcija koristi kada se žele prikupiti „živi“ podaci, tj. podaci koji se mogu iščitati pomoću sučelja samog uređaja. Analiza podataka logičke ekstrakcije puno je brža nego analiza podataka koji su prikupljeni metodom fizičke ekstrakcije. Tijekom provedbe procesa forenzičke analize trajanje analiziranja forenzičke slike stvorene fizičkom ekstrakcijom iznosilo je 12 sati što je u nekim slučajevima i istragama predugo. Veliki izazov za istražitelja je donošenje odluke o tome koja metoda ekstrakcije će biti korištena kako bi se zadovoljili kriteriji integriteta, cjelovitosti i neopovrgnutosti prikupljenih podataka tj. dokaza.

7. Zaključak

Svakim danom broj pametnih uređaja eksponencijalno raste što je vidljivo u svakodnevnim aktivnostima koje su popraćene korištenjem svih vrsta pametnih uređaja. Nedvojbeno je da se pametni telefoni osim za mobilne glasovne pozive koriste i u svrhu slanja tekstualnih poruka te raznih vrsta medija kao što su zvukovni, slikovni i video zapisi što s vremenom kod svakog pojedinog korisnika generira veliku količinu podataka. U slučaju aplikacija za trenutačnu razmjenu poruka zanimljivo je to što je svaki podatak vezan barem za dva korisnika, a u slučaju grupnih razgovora i više. Takvi podaci su vrijedni za izradu i povezivanje vremenskih linija događaja što je za određenu istragu od ključnog značaja.

Kako bi se što vjernije prikazala važnost podataka koje generiraju aplikacije za trenutačnu razmjenu poruka, u ovom diplomskom radu opisane su sve bitne značajke i arhitekture takvih aplikacija. Opisane su i metode ekstrakcije koje su omogućene hardverskim i softverskim alatima tvrtke Hancom koji su kompatibilni sa širokom lepezom Android uređaja, ovom tržištu poznatih i manje poznatih proizvođača.

Postupci koji su provedeni tijekom forenzičke analize u potpunosti su u skladu s metodologijama i procesima koji se koriste u svim ozbiljnim forenzičkim laboratorijima. Samim time posebna pažnja pridodana je postupku prikupljanja podataka i procesu *root*-anja pametnog telefona kako bi softver što uspješnije i cjelovitije prikupio dokaze. Prikupljeni podaci, u istražiteljskom postupku dokazi, analizirani su alatom MD-RED koji implementira razne korisne metode filtracije podataka uz podršku najsuvremenijeg korisničkog sučelja. Navedeni su neki od primjera općenite filtracije podataka, te su slikovno prikazana sučelja određenih kategorija koje softverski alat za analizu podataka posjeduje.

Obavezno je za napomenuti da su alati tvrtke Hancom izuzetno prilagođeni korisniku što podrazumijeva detaljan uvod u rad samog alata, prikazivanje prečica i raznih *čarobnjaka* koji istražitelju omogućuju slikovitiji uvid u postupke analize i obrade podataka, a samim time olakšava izradi vremenskog slijeda događaja.

Korištenje ovakvih suvremenih alata istražitelju uvelike olakšava sami proces prikupljanja podataka, obrade istih te generiranje izvještaja koji su u skladu sa svim prihvaćenim normama i pravilima.

LITERATURA

[1] Sahoo, S. R., Gupta, B. B., Peraković, D., Peñalvo, F. J. G., Cvitić, I. Spammer Detection Approaches in Online Social Network (OSNs): A Survey. In: Knapcikova, L., Peraković, D., Periša, M., Balog, M. (eds) Sustainable Management of Manufacturing Systems in Industry 4.0. *EAI/Springer Innovations in Communication and Computing*. Springer, Cham. 2022. Preuzeto s: https://doi.org/10.1007/978-3-030-90462-3_11 [Pristupljeno: rujan 2024.]

[2] Tang ,Y., Hew, K.F. Effects of using mobile instant messaging on student behavioral, emotional, and cognitive engagement: a quasi-experimental study. *Int J Educ Tehnol High Educ.* 2022;19(3). Preuzeto s: https://doi.org/10.1186/s41239-021-00306-6 [Pristupljeno: rujan 2024.]

[3] Chang, Hui_Jung. Instant Messaging Usage and Interruptions in the Workplace. *International Journal of Knowledge Content Development & Technology*. 2014;4(2): 25-47. Preuzeto s: https://doi.org/10.5865/IJKCT.2014.4.2.025 [Pristupljeno: rujan 2024.]

[4] Statista: Number of smartphone mobile network subscriptions worldwide from 2016 to 2022, with forecast from 2023 to 2028; Dostupno na: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. [Pristupljeno: rujan 2024.]

[5] Simform: App Usage Statistics 2022 that will Surprise You; Dostupno na: https://www.simform.com/the-state-of-mobile-app-usage/. [Pristupljeno; rujan 2024.]

[6] Yulianto, B., Heriyanni, E.Citra Dewi, L., Adinugroho, T. Y. Architecture and Implementation of Instant Messaging in Educational Institution. *Procedia Computer Science*. 2015;59:5-13. Preuzeto s: https://www.sciencedirect.com/science/article/pii/S1877050915018608 [Pristupljeno: rujan 2024.]

[7] Phillips, M. B. The Adventages and Disadventages of AoI Instant Messenger As a Chat Reference System. 2004. Preuzeto s: https://doi.org/10.17615/a4dv-rr52 [Pristupljeno: rujan 2024.

[8] Similarweb: Most Popular Messaging Apps Worldwide 2023; Dostupno na: https://www.similarweb.com/blog/research/market-research/worldwide-messaging-apps/ [Pristupljeno: rujan 2024.]

[9] Long, J., Cvitić, I., Zhang, X. *et al.* Badoo Android and iOS Dating Application Analysis. *Mobile Netw Appl.* 2023; 28: 1272–128. Preuzeto s: https://doi.org/10.1007/s11036-022-02048-9 [Pristupljeno: rujan 2024.]

[10] Bazara, B., Fatma, T. Instant Messaging: Standards, Protocols, Applications, and Research Directions. *Internet Policies and Issues.* 2010. Preuzeto s: https://www.researchgate.net/publication/280307922_Instant_Messaging_Standards_Protocols_Applications_and_Research_Directions [Pristupljeno: rujan 2024.]

[11] Jennings III, R. B., Nahum, E. M., Olshefski, D. P., Saha, D., Shae, Z., Waters, C. A study of Internet instant messaging and chat protocols. *IEEE Network*. 2006; 20:16-21. Preuzeto s: https://www.researchgate.net/publication/3283066_A_study_of_Internet_instant_messaging_and_chat_protocols [Pristupljeno: rujan 2024.]

[12] Umar, A. U., Wakili, A. A Comparative Study of Modern Operating Systems in terms of Memory and Security: A Case Study of Windows, iOS, and Android. *SLU Journal of Science and Technology*. 2023; 6(1 i 2): 131-138. Preuzeto sa: https://www.researchgate.net/publication/371462037_A_Comparative_Study_of_Modern_Operating_Systems_in_terms_of_Memory_and_Security_A_Case_Study_of_Windows_iOS_and_Android [Pristupljeno: rujan 2024.]

[13] Shirota, R., Sakui, K. NAND flash memory created from the very beginning. *JSAP Review.* 2023. Preuzeto s: https://doi.org/10.11470/jsaprev.230103 [Pristupljeno: rujan 2024.]

[14] Samsung Enterprise Mobility Solutions. White Paper: An Overview of the Samsung KNOX Platform. 2015. Preuzeto s: https://kp-cdn.samsungknox.com/df4184593021d7b8fabfdfeff5c318ba.pdf [Pristupljeno: rujan 2024.]

[15] Wilkinson, K., Lyngbaek, P., Waqar, H. The Iris Architecture and Implementation. *IEEE Transactions on Knowledge and Data Engineering 2*, 1990; 1:63–75. Preuzeto s: https://www.academia.edu/76471015/The_Iris_architecture_and_implementation [Pristupljeno: rujan 2024.]

[16] Pedroso, J. E., Tubola, L. F., Aquidado, E. Facebook Messenger: As Means of Communication for Academic Inquiries. *Journal of Digital Learning and Distance Education.* 2023; 2: 491-505. Preuzeto s: https://www.researchgate.net/publication/372771126_Facebook_Messenger_As_Means_of_Communication_for_Academic_Inquiries [pristupljeno: rujan 2024.]

[17] Dong, S., Kryczka, A., Jin, Y., Stumm, M. RocksDB: Evolution of Development Priorities in a Key-value Store Serving Large-scale Applications. *ACM Transactions on Storage.* 2021; 17(4): 1-32. Preuzeto s: https://doi.org/10.1145/3483840 [Pristupljeno: rujan 2024.]

[18] Ntonja, M., Ashawa, M. Examining artifacts generated by setting Facebook Messenger as a default SMS application on Android: Implication for personal data privacy. *Security and Privacy 3.6.* 2020; 3.6: e128. Preuzeto s: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.128 [Pristupljeno: rujan 2024.]

[19] WhatsApp: How we work with the Facebook Companies; Dostupno na: https://faq.whatsapp.com/495458902617269/?locale=hr_HR&eea=1. [Pristupljeno: rujan 2024.]

[20] Ramadhan, M. I., Riadi, I. WhatsApp based Android using National Institute of Standard Technology (NIST) Method. *International Journal of Computer Applications.* 2019; 177(8): 975-8887. Preuzeto s: https://www.researchgate.net/profile/Iqbal-Ramadhan/publication/336656982_Forensic_WhatsApp_based_Android_using_National_Institute_of_Standard_Technology_NIST_Method/links/5daa573d299bf111d4b

e69cd/Forensic-WhatsApp-based-Android-using-National-Institute-of-Standard-Technology-NIST-Method.pdf [Pristupljeno: rujan 2024.]

[21] Ashawa, M., Ogwuche, I. Forensic data extraction and analysis of left artifacts on emulated android phones: a case study of instant messaging applications. *Seizure.* 2017; 2(11): 8-16. Preuzeto s: https://www.researchgate.net/profile/Moses-Ashawa/publication/321961356_Forensic_Data_Extraction_and_Analysis_of_Left_Artifacts_on_emulated_Android_Phones_A_Case_Study_of_Instant_Messaging_Applications/links/6053719192851cd8ce4f6d5f/Forensic-Data-Extraction-and-Analysis-of-Left-Artifacts-on-emulated-Android-Phones-A-Case-Study-of-Instant-Messaging-Applications.pdf?_sg%5B0%5D=started_experiment_milestone&origin=journalDetail [Pristupljeno: rujan 2024.]

[22] Milenković, M., Vojković, G., Rajič, V. Digital forensics appliance in corporate ecosystem considering limitations in the EU legal framework. 2020: 2097-2099. Preuzeto s: https://www.researchgate.net/publication/344463324_Digital_forensics_appliance [Pristupljeno: rujan 2024.]

[23] Milenković, M., Vojković, G., Katulić, T. IoT and Smart Home Data Breach Risks from the Perspective of Croatian Data Protection and Information Security Law. 2019. Preuzeto s: https://www.researchgate.net/publication/335828354_IoT_and_Smart_Home_Data_Breach_Risks_from_the_Perspective_of_Croatian_Data_Protection_and_Information_Security_Law [Pristupljeno: rujan 2024.]

Popis kratica

AMR	Adaptive Multi Rate
DMA	Direct Memory Access
DRK	Device Root Key
DUHK	Device-Unique Hardware Key
EFS	Elastic File System
eMMC	Embedded Multi-Media Controller
eMCP	Embedded Multi-Chip Package
ENISA	The European Union Agency for Cybersecurity
F2FS	Flash-Friendly File System
FAT	File Allocation Table
FPCB	Flexible Printed Circuit Board
FSR	Function Statistics Record
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HFS+	Hierarchical File System Plus
HDMI	High_definition Multimedia Interface
JTAG	Joint Test Action Group
NAND	Not-AND
NSA	National Security Agency
NTFS	New Technology File System
OLAF	*franc*. Office europeen de lutte antifraude (*hrv*. Europski ured za borbu protiv prijevara)
PCB	Printed Circuit Bord
PDF	Portable Document Format
PKM	Periodic Kernel Measurement
RAM	Random Access Memory
RKP	Realtime Kernel Protection
SAK	Samsung Attestation Key

SQL	Structured query language
SSBK	Samsung Secure Boot Key
TAT	Text Attribute Table
USB	Universal Serial Bus
VDFS	VisualSVN Distributed File System
Wi-Fi	Wireless Fidelity
WAV	Waveform Audio File Format
XML	Extensible Markup Language
YAFFS	Yet Another Flash File System

Popis slika

Slika 1. Prikaz najkorištenijih IM aplikacija na uzorku od 100 zemalja 7
Slika 2. Prikaz QR i 60-znamenkastog koda za provjeru enkripcije 16
Slika 3. Znakovi statusa poruke WhatsApp aplikacije 17
Slika 4. Selektivno izdvajanje podataka u MD-LIVE softverskom alatu 23
Slika 5. MD - BOX forenzički alat 26
Slika 6. Odabir modela pametnog telefona 38
Slika 7. Ponuđene vrste ekstrakcije 39
Slika 8. Android Recovery mod 39
Slika 9. Slika zaslona uređaja tijekom odabira postavki za ekstrakciju podataka 40
Slika 10. Parametri pohrane forenzičke slike 41
Slika 11. Izvršavanje procesa ekstrakcije podataka 42
Slika 12. Verifikacija forenzičke slike 42
Slika 13. Generirane datoteke nakon završene logičke ekstrakcije 43
Slika 14. Odabir datotečnih particija 44
Slika 15. Informativni podaci o slučaju 44
Slika 16. MD-RED explorer bočni prozor 46
Slika 17. Filtriranje i sortiranje podataka 50
Slika 18. Poslovni podaci WhatsApp kontakta 50
Slika 19. Opcije filtriranja poruka po vrsti 51
Slika 20. Vizualizacija WhatsApp razgovora 52
Slika 21. Djelomično oporavljene fotografije 52
Slika 22.Vizualizacija Facebook Messenger poruka 53
Slika 23. Kartografski prikaz lokacija 54

Popis tablica

Tablica 1. Popis podataka u tablici *address_table* 13
Tablica 2. Struktura messages tablice WhatsApp msgstore.db baze podataka 18
Tablica 3. Struktura wa_contacts tablice u WhatsApp wa.db bazi podataka 19
Tablica 4. Popis datoteka od interesa za forenzičku analizu WhatsApp aplikacije 20
Tablica 5. Popis alata korištenih u procesu forenzičke analize 36
Tablica 6. Identifikatori pametnog telefona 37
Tablica 7. Popis particija i pripadajuće vrijednosti 45
Tablica 8. Usporedba količine prikupljenih podataka 54

Popis grafikona

Grafikon 1. Broj korisnika pametnih telefona na globalnoj razini od 2012. do 2023. godine ... 4
Grafikon 2. Prikaz prosječnog vremena provedenog koristeći određenu kategoriju aplikacije u jednom tjednu 5

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____diplomski rad _____
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom _____Forenzička analiza aplikacija za trenutačnu razmjenu poruka___ , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, ___19.09.2024.___ Josip Penava_____
(ime i prezime, *potpis*)