Analiza procesa ekstrakcije podataka sa mobilnih uređaja korištenjem forenzičkih metoda u skladu sa zakonskom reglativom

Rajič, Vinko

Undergraduate thesis / Završni rad

2017

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:119:701704

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Vinko Rajič

ANALIZA PROCESA EKSTRAKCIJE PODATAKA S MOBILNIH UREĐAJA KORIŠTENJEM FORENZIČKIH METODA U SKLADU SA ZAKONSKOM REGULATIVOM

ZAVRŠNI RAD

Zagreb, 2017.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 24. travnja 2017.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 3919

Pristupnik: **Vinko Rajič (0135229051)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza procesa ekstrakcije podataka sa mobilnih uređaja korištenjem forenzičkih metoda u skladu sa zakonskom reglativom**

Opis zadatka:

Opisati razvoj forenzičke analize informacijsko-komunikacijskog sustava. Objasniti karakteristike forenzičke analize mobilnih terminalnih uređaja. Dati pregled zakonske regulative područja forenzičke analize terminalnih uređaja. Analizirati mogućnosti primjene forenzičkih metoda u forenzičkoj istrazi.

Zadatak uručen pristupniku: 28. travnja 2017.

Mentor:

Siniša Husnjak, mag. ing. traff.

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

ANALIZA PROCESA EKSTRAKCIJE PODATAKA S MOBILNIH UREĐAJA KORIŠTENJEM FORENZIČKIH METODA U SKLADU SA ZAKONSKOM REGULATIVOM

ANALYSIS OF DATA EXTRACTION FROM MOBILE DEVICES USING FORENSICS TOOLS IN COMPLIANCE WITH LEGISLATION

Mentor: dr. sc. Siniša Husnjak

Student: Vinko Rajič

JMBAG: 0135229051

Zagreb, rujan 2017.

ANALIZA PROCESA EKSTRAKCIJE PODATAKA SA MOBILNIH UREĐAJA KORIŠTENJEM FORENZIČKIH METODA U SKLADU SA ZAKONSKOM REGULATIVOM

SAŽETAK

Forenzika mobilnih uređaja je proces kojim se dobivaju dokazi sa svrhom korištenja u sudskim procesima. Postoji nekoliko bitnijih procesa prilikom sudskog procesa, ali u ovome radu pažnja je prvenstveno usmjerena na proces ekstrakcije podataka i tijek forenzičke istrage. Procesom ekstrakcije podataka dobivaju se informacije koje se kasnije mogu upotrijebiti u sudskom procesu. Zbog raznolikosti mobilnih uređaja, koriste se različiti alati i metode. Osim što se treba paziti na rukovanje s dokazima prilikom dobivanja istih, potrebno je paziti da se ne prekrše procedure i zakoni, kako dobiveni dokazi ne bi bili odbačeni. Proces ekstrakcije podataka je samo dio većeg procesa koji spada pod forenzičku istragu. Forenzička istraga objedinjuje pravnu regulativu i znanstvene metode sa svrhom donošenja ispravne sudske odluke.

Ključne riječi: proces ekstrakcije podataka; zakonska regulativa; dokazi

SUMMARY

Mobile device forensics is a process used to obtain evidence for the purposes of court proceedings. There are several key processes during the court proceeding, but in this paper, attention is primarily directed to the process of data extraction and forensic investigation. The result of using the data extraction process is information that can be later use in court. Due to the variety of mobile devices, various tools and methods are being used. In addition to having to deal with evidence while obtaining it, it is important to keep in mind that the procedures and laws are not violated, so that the obtained evidence would not be rejected. Data extraction process is only a part of a much larger process that is called forensic investigation. Forensic investigation combines legal regulation and scientific methods for the purpose of making a correct court decision.

Keywords: data extraction process; legislation; evidence

Sadržaj

1. Uvod ... **1**

2. Razvoj forenzičkih znanosti ... **3**

2.1. Razvoj digitalne forenzike ... 3

2.2. Uvod u digitalnu forenziku ... 4

2.2.1. Kriminalističke istrage ... 5

2.2.2. Sudski procesi ... 5

2.2.3. Prikupljanje podataka ... 6

2.2.4. Administracija u poduzećima ... 6

3. Forenzika mobilnih terminalnih uređaja ... **7**

3.1. Osnovne komponente mobilnih uređaja ... 7

3.1.1. GSM mobilni uređaji ... 8

3.1.1.1. Softver ... 8

3.1.1.2. Hardver ... 9

3.1.1.3. *Subscriber Identity Module* (SIM) kartica ... 11

3.2. Osnovne forenzike mobilnih uređaja ... 12

3.3. Metode i procesi ekstrakcije podatka ... 14

3.3.1. Metode ekstrakcije podataka ... 15

3.3.1.1. Osnovne metode ekstrakcije ... 16

3.3.1.2. Ostale metode ekstrakcije ... 17

3.3.2. Proces ekstrakcije podatka s mobilnih uređaja ... 18

3.4. Forenzički alati ... 23

3.4.1. Ekstrakcija s Android operativnog sustava ... 23

3.4.2. Ekstrakcija s iOS ... 24

3.4.3. Ekstrakcija s *Windows Phone* ... 24

3.4.4. Ekstrakcija podataka sa SIM kartice ... 25

3.5. Prikupljanje podataka uz suradnju sa operatorom/davateljem usluga ... 27

3.6. Triangulacija mobilnog uređaja ... 28

4. Izazovi prilikom prikupljanja dokaza ... **29**

4.1. Izazovi uzrokovani trenutnim poteškoćama ... 29

4.2. Nezakonito prikupljanje dokaza ... 31

5. Pravna regulativa ... **32**

5.1. Zakon o elektroničkim komunikacijama ... 32

5.2. Zakon o zaštiti osobnih podataka ... 33

5.3. Zakon o kaznenom postupku ... 33

5.4. Europski protu-prijevarni ured (OLAF) 35
6. Tijek istrage 36
6.1. Zapljena uređaja 36
6.2. Prikupljanje dokaza 37
6.3. Analiza 37
6.4. Izvještavanje ovlaštenih institucija 38
7. Zaključak 39
Korištena literatura 40
Popis kratica 45
Popis slika 47
Popis tablica 47
Popis grafikona 47

1. Uvod

Globalizacija i digitalizacija su u današnjem vremenu postala svakodnevnica. Činjenica da informacija uz korištenje mobilnog uređaja može biti prisutna u bilo kojem trenu u bilo kojem dijelu svijeta je zapanjujuća. Međutim, unatoč svim prednostima koje se nude, postoje pojedinci ili organizacije koje će zloupotrijebiti tu mogućnost na štetu ostalih. Kada se izvrši kriminalno djelo, potrebno je reagirati na odgovarajući način, a taj način je korištenjem relativno mladom znanstvenom granom koja se zove forenzika.

Forenzika je znanost kojom se prikupljaju, obrađuju i prezentiraju dokazi pred nadležnim tijelom. Forenzika sama po sebi je širok pojam, te će se u ovom radu orijentirati na samo jednu određenu granu.

Ovaj rad orijentira se na podgranu forenzike koja spada pod digitalnu forenziku, a naziva se forenzika mobilnih uređaja. Forenzika mobilnih uređaja je relativno mlada grana jer je razvoj istih „eksplodirao“ početkom 21. stoljeća. U ovom radu će se pojasniti najbitnije značajke navedene grane. Ovaj rad sastoji se od sedam poglavlja, a to su:

1. Uvod

2. Razvoj forenzičkih znanosti

3. Forenzika mobilnih terminalnih uređaja

4. Izazovi prilikom prikupljanja dokaza

5. Pravna regulativa

6. Tijek istrage

7. Zaključak

U drugom poglavlju obraditi će se razvoj digitalne forenzike kao podgrane te utjecaj razvoja računala i mobilnih uređaja na svijet. Zatim, navedeni su prijelomni trenutci za koje se smatra da su najviše utjecali na razvoj digitalne forenzike te na kojim područjima se ista može primijeniti.

U trećem poglavlju navest će se metode ekstrakcije podataka s mobilnih uređaja te kako funkcionira proces istih. Zatim, navest će se najbitnije komponente uređaja s kojih se mogu dobiti potencijalni dokazi te načini kako se mogu dobiti podaci o okrivljeniku uz suradnju s operatorom.

Sa četvrtim poglavljem su izjašnjene najčešće poteškoće koje mogu nastupiti prilikom prikupljanja dokaza za koje bi forenzičar trebao biti pripremljen; bile te poteškoće izazvane tehničkom ili administrativnom prirodom.

U petom poglavlju nalaze se podaci o zakonskoj regulativi koja se mora provoditi prilikom provođenja istrage. Navedene su najbitnije zakonske stavke koje mogu uvelike utjecati na prikupljanje dokaza kao i na sam ishod suđenja.

Sa šestim poglavljem je objašnjen tijek istrage, točnije gdje forenzičar i forenzički alati ulaze kao dio veće cjeline. Sam proces ekstrakcije podataka je samo manji korak u kompletnom procesu istrage.

Cilj ovog rada je proširiti znanje o forenzici mobilnih uređaja kao i o procedurama koje se izvode kako bi ista mogla proći bez poteškoća. Zatim, cilj je istražiti koje su sve mogućnosti dostupne u sklopu forenzike mobilnih uređaja.

2. Razvoj forenzičkih znanosti

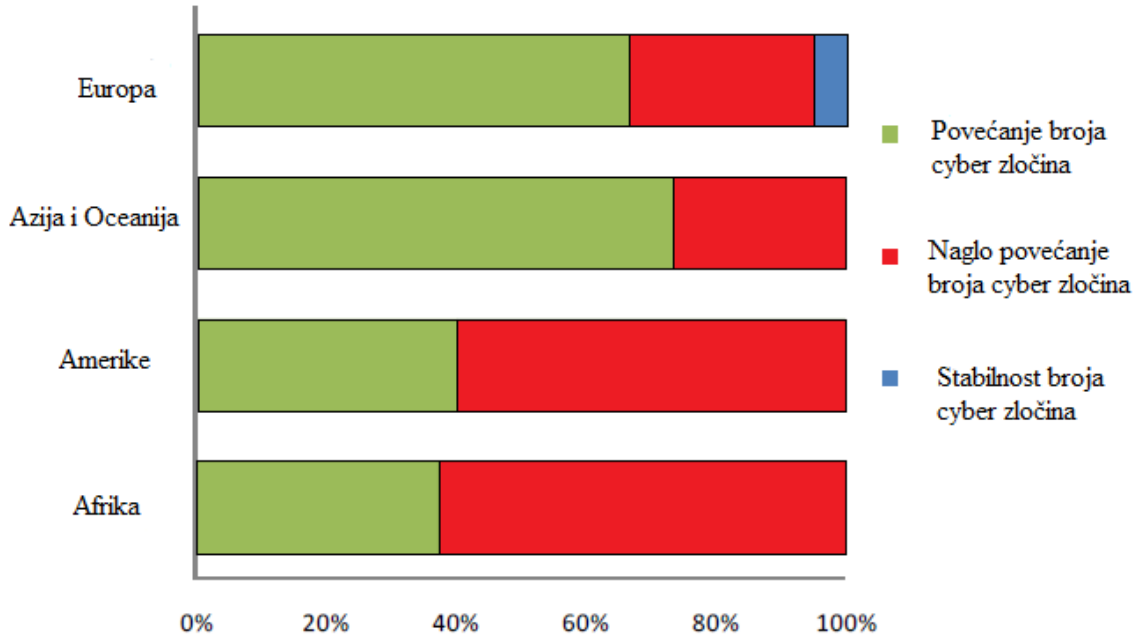
Forenzika podrazumijeva primjenu znanstvenih metoda te zakona od strane odgovarajućih institucija za provođenje kriminalističke istrage. Također, forenzika predstavlja skup aktivnosti i procesa kojim se pronalaze, prikupljaju i interpretiraju fizički dokazi. Ukratko, forenzika predstavlja nijemog svjedoka, točnije fizičke dokaze, kojeg ispituje za to ovlašteno osoblje, [1].

U forenzici, zakonski i znanstveni aspekt su integrirani, tj. ne mogu jedan bez drugoga. Razlog tome jest to što je najbolji forenzički dokaz beskoristan ako je prikupljen ilegalno, [2].

2.1. Razvoj digitalne forenzike

Prije razvoja osnovnih grana forenzike, bilo je vrlo teško odrediti krivca za neko djelo. Razlog tome jest to što su se koristile metode mučenja te je najčešće pobjeđivao onaj s boljim argumentima. Vrlo često se događalo da su pojedinci priznali, iako nisu bili krivi. Iako je digitalna forenzika sama po sebi „mlada“ grana, to ne znači da ona nije kompleksna.

Razvoj digitalne forenzike započeo je sredinom 20. stoljeća s razvojem računala. Primjena prvih računala je prvenstveno bila u industrijskoj proizvodnji u vlasništvu korporacija, instituta, vladinih organizacija i slično. Osnovna zadaća prvih računala bila je procesuiranje podataka. Iako su prva računala imala za današnje standarde slabu procesorsku snagu, ta računala su vršila procesiranje podataka s kojima su organizacije provodile svoje funkcije. Kako bi se izbjegla manipulacija podacima, počela se razmatrati informacijska sigurnost te metode kojima bi se moglo počinitelju ući u trag. Može se reći da je razvoj digitalne forenzike započeo s komercijalizacijom IBM-ovog računala 1980. godine kada se formirala prva organizacija posvećena digitalnoj forenzici koja se zvala IACIS (engl. *International Association of Computer Investigative Specialists*). Nedugo nakon komercijalizacije, počelo se s kriminalnim djelima. U devedesetim godinama 20. stoljeća, došlo je do eksponencijalnog razvoja računala, kao i mobilnih uređaja te je došlo do povećane uporabe interneta. S razvojem tehnologije došlo je do povećanja kriminalnih aktivnosti. Najviše se isticao rast slučajeva s pedofilijom. Prvi značajan razvoj forenzičkih metoda počeo je nakon 11. rujna kada se dogodio teroristički napad na *World Trade Centre*. Razlog tome jest to što nadležne službe nisu bile u mogućnosti predvidjeti napad, iako su se prilikom organizacije čina koristili osnovni načini komunikacije; mobiteli, računala i slično. Osim razvoja metoda, došlo se do zaključka da za primjenu digitalne forenzike trebaju izvršavati ljudi sa dovoljno visokom razinom edukacije, [3].



Grafikon 1: *Cyber* zločini uočeni od zakonodavnih tijela u periodu od 2007. do 2011. godine. Izvor: [4]

Iz grafikona 1 vidljivo je da je najveći porast zabilježen u Africi, a najmanji u Europi. Razlog tome jest to što je u većini Afrike mobilni uređaj „nova" tehnologija, a nasuprot stoji Europa gdje je mobilni uređaj svakodnevnica te je generalna populacija upoznata s opasnostima koje dolaze uz isti.

2.2. Uvod u digitalnu forenziku

Glavna premisa digitalne forenzike jest ta da se svemu može ući u trag. Sa svakim klikom na današnjim terminalnim uređajima ostavljamo digitalni „trag". Taj „trag" može se upotrijebiti kao dokaz prilikom kriminalističke istrage. Primjer toga može biti spajanje s baznim stanicama prilikom počinjenja nekog kaznenog dijela. Digitalna forenzika predstavlja primjenu računalnih i istražiteljskih procedura u svrhu analize digitalnih dokaza koji će se poslije upotrijebiti u svrhu dobivanja informacija o počinitelju nekog dijela.

Digitalna forenzika podrazumijeva puno više od računala i terminalnih uređaja. Pod navedenu disciplinu forenzike spadaju računalne mreže, „*cloud*" sustavi i slično. Digitalna forenzika također podrazumijeva analizu prikupljenih slika, videa i zvuka. Svrha takvih analiza je odrediti, usporediti i pojačati jasnoću koristeći određene metode i alate.

Digitalna forenzika ima više primjena kao što su, [5]:

a. Kriminalističke istrage
b. Sudski procesi
c. Prikupljanje podataka
d. Administracija u poduzećima (npr. ako je netko u poduzeću izvršio nešto ilegalno, digitalna forenzika se koristi za pronalazak krivca)

2.2.1. Kriminalističke istrage

Prilikom spominjanja digitalne forenzike, obično se podrazumijeva da je riječ o krađi identiteta ili dječjoj pornografiji. Iako se takve vrste istrage obično orijentiraju samo na digitalni aspekt istrage, također postoje i drugi načini primjene digitalne forenzike. Koristeći odgovarajuće metode i alate, dokazi se mogu prikupiti u skoro bilo kojem krivičnom dijelu. To podrazumijeva dijela kao što su: ubojstva, pljačke, teroristički činovi, itd., [5].

Najveći problem u digitalnoj forenzici predstavlja nedovoljan broj ovlaštenog osoblja te nemogućnost prepoznavanja takvih dokaza. Ti dokazi mogu podrazumijevati igrače konzole, mobilne uređaje, pametne satove, GPS (engl. *Global Positioning System*), itd. Osim toga, metode enkripcije postaju sve sofisticiranije što značajno može otežati prikupljanje bilo kakvog korisnog dokaza. Uz to, drugu najveću prepreku predstavljaju zakonska ograničenja prilikom pribavljanja dokaza. Jedinu prednost koju istražitelji imaju u sklopu istrage jest ta da većina osumnjičenika nisu svjesni da nakon brisanja datoteka, podaci ostaju prisutni još neko vrijeme. Razlog zašto je bitan razvoj digitalne forenzike jest to zato što se na taj način mogu spriječiti zločini prije nego što se dogode. Primjerice, može se spriječiti regrutiranje pojedinaca u terorističku organizaciju; zatim, pripremiti „zamku“ za seksualne prijestupnike, itd., [6].

2.2.2. Sudski procesi

Korištenje digitalne forenzike u civilnim parnicama u današnjim uvjetima predstavlja unosan posao. Godine 2011. procijenjeno je da je oko 780 milijuna dolara dobiveno samo iz civilnih parnica. Kao dio procesa koji se zove *eDiscovery*, digitalna forenzika predstavlja najbitniju komponentu prilikom sudskih parnica. *eDiscovery* podrazumijeva sve procese koji se upotrjebljavaju prilikom prikupljanja, analize, osiguravanja dokaza koji se kasnije mogu iskoristiti u parnici, [5].

U civilnim parnicama, obje strane imaju pravo na pregled dokaza koji će biti iskorišteni protiv njih prije samog suđenja. Najčešći slučajevi kod civilnih parnica su rastava braka ili borba za skrb nad djecom. Civilne parnice su karakteristične zato što se dokazi najčešće prikupljaju prije nego što se krene sa sudskim postupkom. Razlog tome jest taj da pojedinci žele prikupiti što više dokaza kako bi imali pogodniju argumentaciju za sudsku parnicu. Jedan od primjera prikupljanja dokaza jest korištenje *keylogger*-a. *Keylogger* je alat koji omogućuje nadzor aktivnosti na računalu; točnije lozinke, povijesti pretraživanja i slično. Alat kao takav je prvenstveno namijenjen za poslovne svrhe za nadzor radnika, ali je praksu našao i u privatnoj primjeni, [7].

2.2.3. Prikupljanje podataka

Razvoj tehnologije ima značajan utjecaj na svakodnevni život. Unatoč brojnim prednostima, taj isti napredak se može zloupotrijebiti. Pod to se podrazumijeva da se novijim i inovativnijim načinima komunikacije sve teže ulazi u trag prilikom kriminalističke istrage.

Primjerice; u terorističkom napadu u Parizu u studenom 2015. godine, u kojem je poginulo preko sto ljudi, saznalo se da su teroristi pri organizaciji terorističkog čina koristili „chat“ PlayStation 4 igrače konzole. Kao što je prethodno napomenuto, zbog takvih „inovacija“, sve se teže ulazi u trag raznim počiniteljima. Iz tog razloga, potrebno je razviti pravilne načine prikupljanja podataka, [8].

Prikupljanje podataka sastoji se od dva dijela. Prvi se dio tiče dostave podataka u forenzičkom slučaju, a drugi dio se temelji na primjeni forenzičkih metoda. Forenzički slučajevi se mogu gledati kao proces čiji su glavni produkti informacije koje koriste ovlaštene institucije, [9].

2.2.4. Administracija u poduzećima (Forenzičko računovodstvo)

Osim primjene digitalne forenzike kod sudskih parnica te nacionalne sigurnosti, ista se može primijeniti ukoliko se izvrši povreda politike ili procedure poduzeća. Povreda se može izvršiti na razne načine, kao što je otkrivanje podataka konkurenciji, namjerna ili nenamjerna sabotaža i slično. U takvim se slučajevima koristi digitalna forenzika kako bi se utvrdilo gdje je „propust“ nastupio. „Propusti“ ne moraju biti nužno protuzakoniti, ali ako se kose s politikom poduzeća, tada nastupaju sankcije od strane poslodavca. Forenzičko računovodstvo se prvenstveno orijentira na računovodstvene prijevare i porezne prijevare. Glavni cilj jest uočavanje nepravilnosti i predaja dopisa ovlaštenim institucijama, [5].

Također, postoje priručnici/načela kojih bi se poduzeća trebala pridržavati. Neka od tih načela su [10]:

- Organizacije/poduzeća trebaju osigurati da njihova sigurnosna politika mora imati jasno definirane pravilnike koji se odnose na mobilne uređaje
- Organizacije/poduzeća bi trebala stvoriti procedure te ih se pridržavati za provođenje forenzike na mobilnim uređajima
- Organizacije/poduzeća bi trebala osigurati da njihovi pravilnici i procedure podupiru razumnu upotrebu forenzičkih alata
- Organizacije/poduzeća bi trebala osigurati da forenziku na uređajima provodi za to ovlašteno osoblje.

3. Forenzika mobilnih terminalnih uređaja

Forenzika mobilnih terminalnih uređaja je dio digitalne forenzike koji se orijentira na mobilne uređaje. Neki od tih uređaja su mobiteli, smartphone uređaji, PDA, iPod, fotoaparati, itd. Takvi mobilni terminalni uređaji su postali neizostavan dio ljudske svakodnevnice te je neizbježna činjenica da će biti korišteni kao alat u kriminalnim aktivnostima. Međutim, prije nego što se nastavi s obrazloženjem forenzike mobilnih uređaja, prvo se mora razumjeti način funkcioniranja mobilnih uređaja, a to će se objasniti u sljedećim poglavljima.

3.1. Osnovne komponente mobilnih uređaja

Postoje više vrste mobilnih uređaja, a najzastupljeniji su [11]:

- CDMA mobilni uređaji
- GSM mobilni uređaji
- iDEN mobilni uređaji

GSM (engl. *Global System for Mobile Communications*) uređaji su jedni od najzastupljenijih vrsta uređaja, a najbitnija stavka ove tehnologije je SIM kartica. SIM kartica omogućava povezivanje uređaja s davateljem usluge, tj. omogućuje korisniku da koristi uređaj te njegove funkcionalnosti. SIM kartica služi kao identifikacija kako bi se korisnik mogao spojiti na mrežu. GSM uređaji su „fleksibilni“, tj. korisnik može birati davatelja usluge bez da mijenja uređaj, [12].

CDMA (engl. *Code-division multiple access*) uređaji se najčešće koriste u SAD-u i Rusiji, iako je u tim zemljama prisutna GSM tehnologija. Navedeni uređaji ne koriste SIM karticu te je svaki uređaj vezan uz davatelja usluga kod kojeg je uređaj kupljen. To znači da je korisnik, ukoliko želi koristiti usluge nekog drugog operatora, prisiljen kupiti uređaj kod drugog operatora, [13].

iDEN (eng. *Integrated Digital Enhanced Network*) je vrsta tehnologije koja omogućava jednostavniju i bržu komunikaciju između korisnika. Unatoč tome, ova vrsta uređaja se istiskuje s tržišta te se integrira s trenutno najzastupljenijim tehnologijama; CDMA i GSM, [14].

Budući da se na hrvatskom području koriste samo GSM uređaji, dalje u radu će se razmatrati samo ta tehnologija.

3.1.1. GSM mobilni uređaji

GSM uređaj ili pametni uređaj je laički rečeno, računalo u džepu. Isti je ostavio neizostavan trag u ljudskoj svakodnevnici te se ne može zamisliti dan bez aparata. Iako omogućuje veliki niz prednosti, istovremeno se njihova učinkovitost može zloupotrijebiti. Prije nego što se krene u obrazloženje forenzičkih metoda i postupaka, mora se razumjeti kako mobilni uređaj funkcionira.

Svaki mobilni uređaj ima svoj IMEI (engl. *International Mobile Equipment Identity*). IMEI je jedinstveni petnaestoznamenkasti broj koji služi za identifikaciju uređaja te se može upotrijebiti ukoliko je uređaj ukraden. Isti se nalazi ispod baterije ili na originalnom pakiranju uređaja te se može vidjeti u postavkama uređaja, [15].

Najbitnije komponente GSM uređaja su softver, hardver, SIM kartica.

3.1.1.1. Softver

Softver je programski kod koji služi za upravljanje hardverom. Također, ima za cilj uskladiti rad svih elektroničkih komponenti. Softver se sastoji od dvije komponente, a to su operativni sustav i aplikacije, [16].

Operativni sustav je skup složenih programskih kodova koji upravlja svim ostalim programima/aplikacijama u računalnom sustavu. Osim toga, operativni sustav vodi kontrolu korištenja resursa u računarskom sustavu i kontrolu izvođenja programa/aplikacija. Osnovne funkcije operativnog sustava su: pokretanje uređaja, izvođenje aplikacija, uporaba memorije i sl., a glavni je cilj pojednostaviti korištenje mobilnog terminalnog uređaja i omogućiti produktivnu uporabu komponenti istog. Osim toga, pokušava se omogućiti uspješna sinkronizacija i koordinacija svih aktivnosti unutar terminalnog uređaja, kao što je gašenje/pokretanje, upravljanje programima/memorijom i slično, [17].

Na mobilnim terminalnim uređajima postoje dvije vrste operativnih sustava, a to su [18]:

- Zatvoreni operativni sustav
- Otvoreni operativni sustav

Zatvoreni operativni sustav je zadužen za direktno upravljanje hardverom terminalnog uređaja i osnovnim operacijama. Takav operativni sustav je posebno osmišljen za hardver uređaj na kojem se nalazi. Primjer takvih sustava su iOS, BlackBerry, itd.

Otvoreni operativni sustav je sustav koji je osmišljen za izvedbu na višestrukim platformama. Takav sustav omogućuje prenošenje i izvođenje aplikacija na uređajima različitih modela, neovisno o proizvođaču. Primjeri takvih sustava su Symbian, Android, WindowsPhone, itd., [18].

Aplikacije su programi osmišljeni kako bi se koristili na mobilnim terminalnim uređajima. Aplikacije mogu biti instalirane od strane proizvođača kao što su internet pretraživači, kalendari, aplikacija za orijentaciju i slično. Takve aplikacije su integrirane i u većini slučajeva se ne mogu obrisati, [19].

Zbog aplikacija koje nisu instalirane od strane proizvođača, proizvođači su omogućili korisnicima skidanje aplikacija preko distribucijskih platformi. Takve platforme su se počele pojavljivati s pojavom pametnih uređaja. Takve platforme su: *App Store*, *Google Play*, *Windows Phone Store* i *BlackBerry App*. Kako bi aplikacija bila kompatibilna s uređajem, proizvođači moraju uzeti u obzir velik broj zahtjeva koje moraju zadovoljiti. Zbog toga, aplikacije mogu biti jednako raznovrsne kao i sami uređaji, što dodatno može otežati posao forenzičara, [18].

3.1.1.2. Hardver

Zbog sve većeg tehnološkog napretka, proizvođači mobilnih terminalnih uređaja su razvili mogućnost spajanja elektroničkih elemenata na jednom jedinstvenom čipu. Taj se čip zove SoC (engl. *System on a Chip*). Sve elektroničke komponente neophodne za rad uređaja nalaze se na sve manjoj površini. Sa stalnim razvojem elektroničkih komponenti, one su sve manje, što je rezultiralo s povećanjem tehnoloških mogućnosti koje su implementirane u mobilne uređaje. Također, postignuta je optimizacija komponenti što je rezultiralo smanjenjem potrošnje energije, povećava se brzina razmjene informacija između komponenti te se smanjuju troškovi hardverskog dizajniranja, [20].

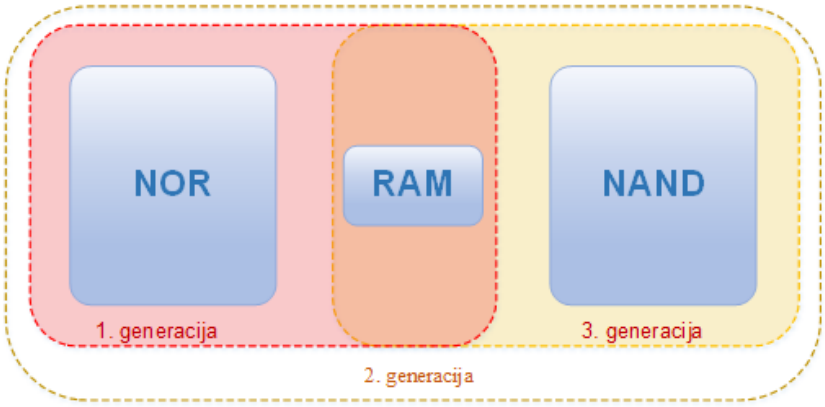
SoC se sastoji od [20]:

- CPU (Central procesorska jedinica)
- GPU (Grafička procesorska jedinica)
- Pripadajuća memorijska kontrola
- Periferni uređaji
- Zaslon

CPU (Centralna procesorska jedinica) ili samo procesor je glavno elektroničko sklopovlje računala. CPU je "mozak" računala te ima funkciju nadzora i upravljanja radom računala, tj. mobilnog uređaja. Sastavljen je od aritmetičko-logičke jedinice, upravljačke jedinice i registara (priručne memorije). Procesor se može sastojati od više jezgri na jednom čipsetu što omogućuje obavljanje više zadataka odjednom, smanjenje radnog takta pojedinih jezgri te smanjenje zagrijavanja i potrošnje energije. Moderni pametni uređaji mogu raditi nekoliko dana ili čak tjedana prije nego što se ugase. Iz tog razloga, CPU je napravljen da omogući dugotrajnost i obavljanje više zadaća istovremeno, [21].

GPU (Grafička procesorska jedinica) je mikroprocesor namijenjen brzom procesuiranju grafičkih informacija. Počeo se implementirati u mobilne terminalne uređaje zbog povećanja kompleksnijih video igara na prijenosnim uređajima, [22].

Memorija mobilnih uređaja jedna je od bitnijih komponenti jer se na njoj nalaze sami podaci. Memorija mobilnih terminalnih uređaja dijeli se na radnu (potrebno napajanje da se ne izgube podaci) i trajnu (neizbrisiva, ne ovisi o napajanju) memoriju. Mobilni uređaji u većini slučajeva imaju jednu ili dvije vrste trajne *flash* memorije, a to su NOR (poput memorije računala) i NAND (poput hard disk-a). NOR omogućava brže učitavanje, ali sporije pohranjuje od NAND memorije. Teško se kvari i blokira. NAND omogućava veće memorijske kapacitete, ali je manje stabilna od NOR memorije te dozvoljava samo sekvencijalni pristup. Današnji pametni uređaji sadrže samo NAND i RAM memorije zbog sve više zahtjeva za većom brzinom prijenosa podataka, [20].



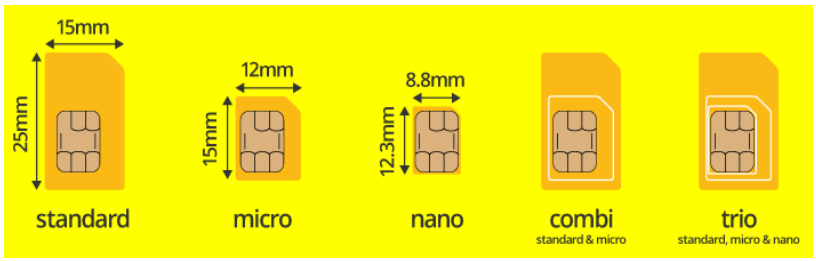
Slika 1: Konfiguracija *flash* i radne memorije po generacijama, [19]

RAM (engl. *Random Access Memory*) memorija je teška za ekstrakciju zbog njezine nestabilne prirode te služi za izvršavanje aplikacija. To znači da će se podaci koji su na njoj izgubiti, ukoliko uređaj izgubi napajanje. NOR memorija vrši pohranu operacijskog sustava, jezgre, računalnih drivera, itd. NAND memorija sadrži podatke kao što su slike, zvukovi, video, itd. S navedene vrste memorije se najviše vrši ekstrakcija podataka, [23].

3.1.1.3. *Subscriber Identity Module* (SIM) kartica

Pametni uređaji koji koriste GSM tehnologiju koriste SIM (engl. *Subscriber Identity Module)* karticu. Ista se koristi za verifikaciju korisnika te spajanje na mrežu davatelja usluge. Spajanjem na mrežu, vrši se pohrana podataka o lokaciji na samu karticu. Osim toga, na SIM kartici se mogu nalaziti podaci kao što su: kontakti, lista poziva, postavke za omogućavanje usluge. SIM kartica omogućava pružanje usluga na mobitelu (pozivi, SMS, MMS, itd.). Može se reći da bez SIM kartice, uređaj nije u mogućnosti pružiti svoj puni kapacitet funkcionalnosti.

SIM kartica dolazi u nekoliko različitih formata (klasični, micro i nano). Također je moguće staviti SIM karticu u drugi uređaj te dalje koristiti istog davatelja usluge, [24].



Slika 2: Različiti formati SIM kartice, [25]

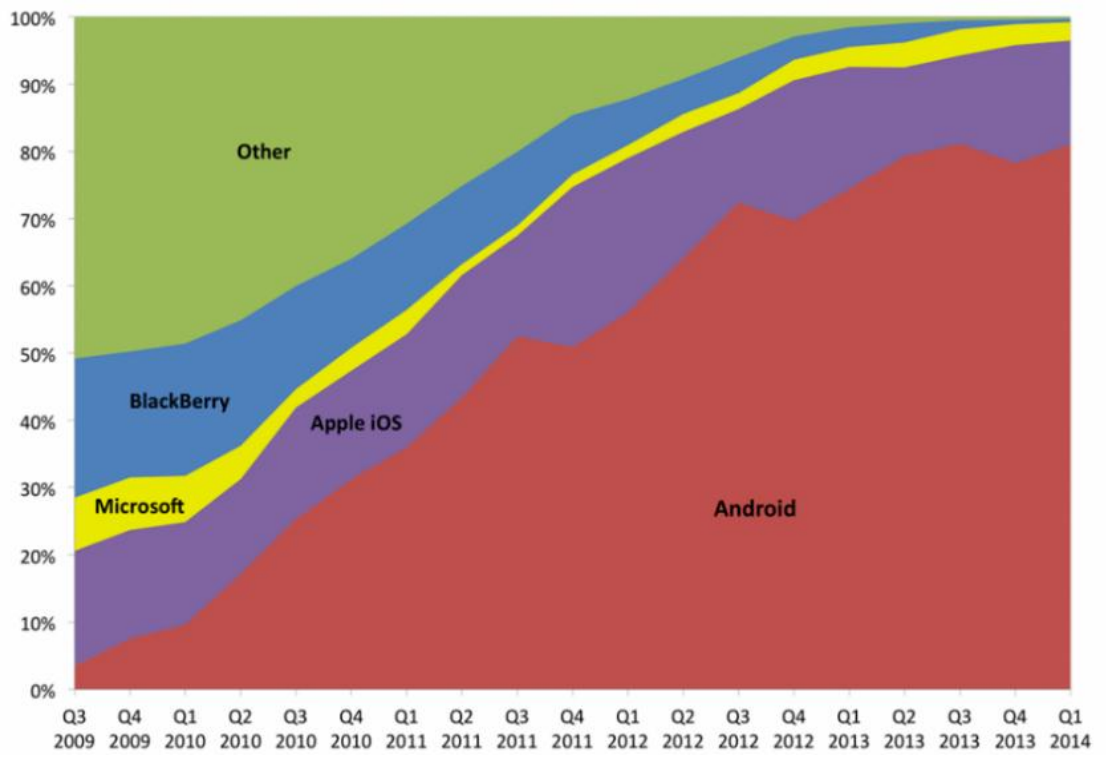
Sama SIM kartica sastoji se od nekoliko ključnih komponenti, a one su mikroprocesor, ROM (engl. *Read-only memory*) i RAM memorije, koji omogućuju pohranu i obradu podataka. Podaci koji se nalaze na SIM kartici uključuju: ICC-ID (engl. *Integrated Circuit Card Identifier*), IMSI, ključ za autentifikaciju, SMS (engl. *Short Message Service*) poruke te kontakte.

ICC-ID sastoji se od koda zemlje, koda mreže te serijski broj SIM-a. Isti je jedinstven za svaki SIM te služi za identifikaciju same kartice. Zatim, IMSI služi za identifikaciju korisnika na mreži te je jedinstven za svakog korisnika. IMSI se sastoji od koda zemlje, koda davatelja usluge te broja korisnika. Ključ za autentifikaciju služi za verifikaciju SIM kartice na mrežu. Svaka SIM kartica ima jedinstveni ključ te se nalazi u memoriji samog uređaja, [26].

3.2. Osnove forenzike mobilnih uređaja

Mobilni uređaji su specifični zato što se u njima nalazi znatno više privatnih podataka nego u primjerice računalima, laptopima i slično. Razlog tome to što svaki uređaj ima jednog korisnika, a ne više kao što to imaju računala, igrače konzole i slično. Mobilni terminalni uređaji najčešće sadrže privatne informacije kao što su lista poziva, poruke, mailovi, multimedijalni sadržaj, brojevi bankovnih računa, itd.

Zbog sve većeg napretka uređaja, također se omogućuje sve veći prijenos podataka kao i povećanje mogućnosti mobilnih uređaja. Takav napredak tehnologije otvara sve veće mogućnosti za zlouporabu od strane kriminalaca. Upravo zbog tog napretka i sve veće količine podataka na uređajima, mogu se lakše pronaći informacije koje će biti potrebne prilikom određivanja krivca nekog kriminalnog djela, primjerice, korištenje mobilnih uređaja kod razbojstava, organizacije terorističkih napada, krijumčarenje robe, itd. Neki uređaji imaju dodatne mogućnosti kao što su mjerenje voltaže, temperature, ubrzanja. Iako su takvi senzori integrirani u uređaj sa svrhom unapređenja doživljaja korisnika, ti se isti senzori mogu zloupotrijebiti za aktivaciju bombi, krađu podataka sa drugih uređaja, [27].



Grafikon 2: Tržišni udio pametnih uređaja sortiranih po platformi, [28]

Tržište mobilnih uređaja je dinamičan sustav. Kao što je prikazano na grafikonu 2, u zadnjih se nekoliko godina povećao broj Android operativnih sustava, a i s njime veći broj pametnih telefona. Karakteristika dinamičnosti se može očitovati u tome da se svaki tjedan izbaci bar pet novih modela uređaja. Iako je to dobra stvar što se tiče marketinga i povećane konkurentnosti na tržištu, s perspektive forenzičkih istražitelja, to predstavlja problem. Problem se očituje u tome što je postalo nemoguće stvoriti jedinstveni alat/metodu za sve uređaje, [29].

Uređaji koji se koriste u svakodnevnici su jedinstveni zbog podataka koji se mogu dobiti iz njih. Razlog tome jest taj da se uređaji spajaju na različite vrste mreža (Telekomunikacijska mreža, LAN, *bluetooth*, itd.) preko kojih se razmjenjuju podaci. Ta količina podataka je u konstantom porastu. Uz sve to, podaci su sami po sebi osjetljivi. To znači da se vrlo lako mogu izgubiti nestručnim rukovođenjem. Također, jedna od mogućnosti jest da se sadržaj uređaja može izbrisati daljinskim putem, [27]. Npr. Apple nudi mogućnost brisanja podataka sa iPhone-a koristeći *iTunes* na računalu. Način na koji funkcionira ta mogućnost je sljedeći; Apple prilikom konfiguracije uređaja zahtijeva da se unesu korisnički podaci (*AppleID*). Koristeći te iste podatke, vlasnik uređaja može putem računala daljinski izbrisati podatke s mobilnog uređaja, [30].

Većina kriminalnih aktivnosti uključuje neku vrstu terminalnog uređaja. Sa sve većim razvojem mobilnih uređaja, isti postaju sve prisutniji u kriminalnim aktivnostima. Postoje četiri načina na koja mobilni uređaj može biti uključen u kriminalnu aktivnost, a to su [31]:

- Može se koristiti kao komunikacijsko sredstvo prilikom kriminalne aktivnosti
- Na samom uređaju se može nalaziti medij (slika, video) koji može biti upotrijebljen kao dokaz
- Može sadržavati žrtvine informacije
- Može biti upotrijebljen kao sredstvo za počinjenje zločina

3.3.Metode i procesi ekstrakcije podataka

Mobilni uređaji postali su mala računala u džepu. Ti uređaji se mogu spajati na različite mreže. Kako bi podaci prije same ekstrakcije ostali netaknuti, uređaj se mora izolirati od tih mreža. Međutim, to ponekad ili nije moguće ili je sama izolacija neuspješna. Pod izolacijom se podrazumijeva stavljanje uređaja u „airplane mode“, gašenje WLAN-a, gašenje mobilnih podataka, micanje SIM kartice iz uređaja, ali najznačajnije metode izolacije su stavljanje uređaja u Farraday-ev kavez/vrećicu te mrežni prigušivač (*cellural jammer*), [32].



Slika 3: Farraday-ev kavez/vrećica, [33]

Na slikama 3 i 4 je vidljiva oprema koja se može iskoristiti za izolaciju uređaja. Farraday-ev kavez izolira uređaj na način da se aparat prvo stavi u vrećicu te vrećica sprječava dotok električnih signala. Mrežni prigušivač onemogućuje spajanje uređaja na mrežu na način da kreira smetnje na istoj frekvenciji na kojoj se mobilni uređaj spaja na mrežu, [32].



Slika 4: Mrežni prigušivač, [34]

Nakon izolacije uređaja, kreće se sa procesom ekstrakcije podataka. Ekstrakcija podataka je proces izvlačenja podataka raznim metodama iz mobilnog uređaja koristeći za to predviđene alate. Podaci koji se izvuku se dalje koriste kao dokazi u kriminalističkom djelu.

3.3.1. Metode ekstrakcije podataka

Prilikom određivanja prikladne forenzičke metode za ekstrakciju podataka, koriste se određeni kriteriji kojima se utvrđuje koja će se metoda koristiti. Taj način određivanja je koristan zato što služi za kategorizaciju forenzičkih alata po njihovoj mogućnosti da izvlače različite količine podatke. U prilogu je vidljiva piramida koja označava forenzičke metode za ekstrakciju podataka. Kako se kreće sa dna piramide (Ručna ekstrakcija) prema vrhu (*Micro Read*), povećava se kompleksnost same ekstrakcije podataka, [35].

To se može očitovati u [35]:

- Što je metoda viša na piramidi, to ona postaje teža za „opravdati/obrazložiti“
- Alati postaju skuplji
- Metode postaju tehnički zahtjevnije
- Dulje je vrijeme potrebno za analizu
- Potrebno je više edukacije za osobu koja vrši ekstrakciju
- Ulaze „dublje“ u uređaj te izvlače više podataka



Slika 5: Metode ekstrakcije podataka. Izvor: [36]

3.3.1.1. Osnovne metode ekstrakcije

Ručna ekstrakcija uključuje pregled podataka koji su pohranjeni na mobilnom uređaju. Kako bi se pristupilo sadržaju, potrebna je ručna manipulacija uz pomoć fizičkog sučelja. To znači da se pregled izvršava na isti način na koji korisnik upotrebljava uređaj. Sam pregled se snima ili fotografira koristeći kameru/fotoaparat. Osim toga, uređaj se može spojiti na računalo, te se pomoću odgovarajućeg programa na računalu snimaju aktivnosti koje forenzičar provodi. Koristeći ovu metodu, nemoguće je povratiti izbrisane podatke. Postoje alati koji omogućuju forenzičaru da prikupi i kategorizira snimljene podatke značajno brže. Unatoč tome, ako postoji velika količina podataka za obraditi, ručna ekstrakcija podataka može potrajati te podaci mogu biti „kontaminirani" ili izbrisani. Ako je zaslon oštećen ili ga u potpunosti nema, ručna ekstrakcija podatka postaje teška ili nemoguća. Osim toga, izazov može predstavljati ako je jezik na uređaju stran istražitelju, [23].

Logička ekstrakcija je proces povezivanja mobilnog uređaja s forenzičkom radnom stanicom koristeći bežičnu ili žičnu vezu. Forenzičar bi trebao biti svjestan problema koji se javlja prilikom odabira metode povezivanja uređaja s forenzičkim alatom. Razlog tome jest taj što podaci mogu biti izmijenjeni ako se ne odabere ispravna metoda povezivanja. Logička ekstrakcija podataka počinje na način da se šalje niz „zapovijedi/kodova" preko sučelja forenzičkog alata na mobilni uređaj. Nakon toga, mobilni uređaj vraća povratnu informaciju kao odgovor na „kod/zapovijed". Odgovor se šalje na radnu stanicu te prijavljuje za daljnju obradu. Logička ekstrakcija podrazumijeva prikupljanje podataka kopirajući bitove s logičke pohrane. Podaci koji se pribavljaju uključuju datoteke koje se nalaze na logičkoj memoriji, [37].

Hex Dumping se provodi učitavanjem prilagođenog programa za učitavanje operacijskog sustava (*boot loader*) u zaštićeni dio memorije. Učitavanje navedenog programa ostvaruje se povezivanjem uređaja na „*flasher box"* koja je onda spojena sa forenzičkim terminalnom. „*Flasher box*" se može gledati kao pomoćni alat jer omogućava pristup podacima. Nizom zapovjednih kodova, „*flasher box*" stavlja uređaj u stanje dijagnostike. Kad je uređaj u tom stanju, „*flasher box*" kopira podatke i prosljeđuje ih na forenzički terminal, [38].

JTAG (engl. *Joint Test Action Group*) je standard podržan od strane proizvođača kojim je definirano da se na uređaje implementira jedinstven ulaz sa svrhom uklanjanja grešaka na memoriji, procesorima i čipovima. Zbog tog standarda, moguće je pristupiti podacima na uređaju preko posebnih priključaka koji se zovu TAP (engl. *Test Access Ports*). JTAG se koristi kada je potrebno zaobići zaštitu na uređaju (pin, lozinka i sl.). Međutim, prije korištenja metode, potrebno je prvo komponentu fizički izvaditi iz uređaja kako bi se mogla izvršiti ekstrakcija, [39].

Chip-Off metoda se odnosi na prikupljanje podataka direktno iz *flash* memorije uređaja. To znači da se *flash* memorija prvo mora fizički ukloniti iz uređaja. Navedena metoda omogućuje istražitelju da stvori binarnu „sliku“ izvađene memorije. Nakon toga, „slika“ se analizira i predaje na daljnju obradu. Prednost ove metode može se očitovati u tome da se zaobilazi zaštita koja je postavljena u uređaju. Zbog različitih vrsta čipova, ova metoda ekstrakcije podataka je vrlo kompleksna te je potrebna velika razina znanja i iskustva za izvođenje, [40].

Micro Read je metoda koja se temelji na snimanju fizičkog pregleda NAND ili NOR čipova sa korištenjem mikroskopa. Zbog same kompleksnosti, ova metoda se najčešće koristi u slučajevima u kojima je ugrožena nacionalna sigurnost i slično. Ova metoda zahtijeva tim istražitelja s odgovarajućom opremom, [23].

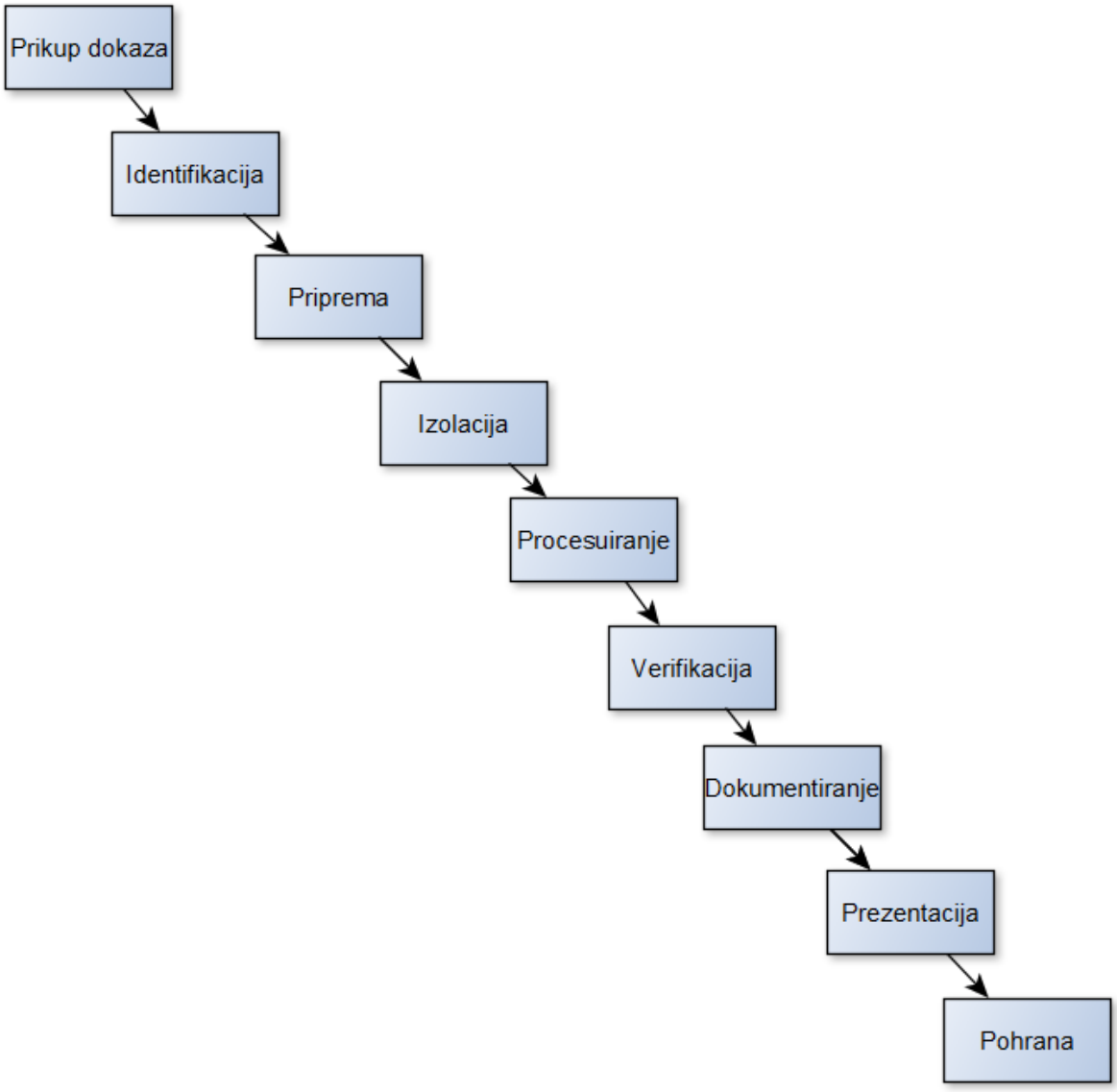
3.3.1.2. Ostale metode ekstrakcije

Cloud computing ili „usluga u oblaku“ je nova tehnologija koja omogućuje davanje usluga putem interneta. Pomoću te tehnologije omogućava se pohrana podataka i programa na internetu umjesto na računalu. Time se izbjegava izgradnja fizičke infrastrukture za pohranu velike količine podataka. Također, navedena tehnologija omogućuje pohranu podataka direktno s mobilnog uređaja. Kada se podaci ne mogu dobiti s uređaja jer je primjerice uređaj uništen, a zna se da je uređaj povezan sa *cloud*-om, moguće je napraviti ekstrakciju podataka s *cloud*-a, ali samo uz odobrenje od davatelja usluge. Ova vrsta tehnologije se najčešće koristi za pohranu ilegalnih podataka kao što je dječja pornografija itd. Problem kod ekstrakcije podataka s ove tehnologije nastaje zbog nedostupnosti i nemogućnosti verifikacije podataka, [41].

Datotečna ekstrakcija omogućava ekstrakciju podataka koji su pohranjeni na SQLite baze podataka. Kada se podaci pohranjuju, podatak zauzima memoriju dok pojedinac ne odluči obrisati istu. Sama adresa tog podatka se u tom trenu smatra zauzetom. Međutim, kada pojedinac odluči obrisati taj podatak, briše se samo adresa, dok sam podatak ostaje nepromijenjen. Iako nije obrisan, podatak će prilikom pohrane neke druge informacije biti zamijenjen. To znači, kada se podaci obrišu, dostupni su samo oni koji nisu zamijenjeni, [37].

3.3.2. Proces ekstrakcije podataka s mobilnih uređaja

Iako je tržište preplavljeno s velikim brojem uređaja i proizvođača istih, za uspješnu ekstrakciju podataka uvijek se može pratiti proces koji je prikazan slikom:



Slika 6: Proces ekstrakcije podataka. Izvor [42]

Kada se vrši ekstrakcija podataka, mora se paziti da se ne prekrše ovlasti koje sudionik u istrazi ima. Kako se to ne bi dogodilo, postavljene su procedure i pravila. Slikom 6 je prikazana metodologija procesa ekstrakcije podataka s mobilnih uređaja. Forenzičar je dužan pratiti na slici navedene korake kako bi što efikasnije i brže izvršio ekstrakciju podataka. Navedena metodologija je samo jedan proces koji se odvija u kompletnoj kriminalističkoj istrazi te i će se sta bolje objasniti u poglavlju 6.

- Prikupljanje dokaza

Prikupljanje dokaza uključuje procedure po kojima se upravlja zahtjevima za pregledom uređaja. Navedeni korak prvenstveno se odnosi na pisane zahtjeve te ostalu administraciju koja se mora provesti preko ovlaštenih institucija. Ova faza služi za dokumentaciju o vlasništvu uređaja, u kakvom „incidentu“ je uređaj bio uključen te koje se točno informacije traže. Najbitniji dio ove faze jest razvoj pojedinih ciljeva za različite preglede i analize, što znači da nisu svi zahtjevi za ekstrakcijom podataka isti te se mogu razlikovati u količini podatka, sadržaju, itd. Vrlo je bitno odrediti koje su informacije potrebne jer ako dođe do krive interpretacije zahtjeva i ekstrakcije pogrešnog podataka, dokaz se neće moći uzeti u obzir, [43].

- Identificiranje

Nakon što se izvrši postupak prikupljanja dokaza te se odredi koji se podaci moraju naći, mora se izvršiti identifikacija samog uređaja. Forenzički istražitelj mora biti u mogućnosti identificirati [35]:

a) Ovlaštene institucije
b) Ciljeve pregleda uređaja
c) Model uređaja te podatke s uređaja
d) Dinamičnu memoriju
e) Ostale potencijalne dokaze

a) Ovlaštene institucije

Zakoni koji se odnose na pregled podataka u mobilnim uređajima svakodnevno se mijenjaju. Vrlo je bitno da forenzičar prati smjernice iz dobivenog naloga za ekstrakcije podataka. To znači da se na samom nalogu stavljaju ograničenja, tj. na nalogu je vidljivo koji su podaci potrebni te se samo njih smije izvući iz uređaja. Može se dogoditi da se traže samo određene informacije. Međutim, moguće je da se ti podaci ne mogu dobiti drugačije nego izvlačenjem drugih podataka koji nisu propisani nalogom, [43].

b) Ciljevi pregleda uređaja

Glavni ciljevi prilikom ekstrakcije podataka se mogu razlikovati. Osim toga, može doći do ograničenja zbog nedostatka opreme ili stručnog osoblja. Iz tog razloga, korisno je da se identificira razina ekstrakcije podatka. Moraju se uzeti u obzir dva parametra: način na koji se dokumentiraju podaci te do koje „dubine“ pregled/ekstrakcija treba biti. Također, može se dogoditi da krivac nije počinio nikakve značajne prekršaje ili je uređaj žrtvin, pa se ekstrakcija podataka može izvršiti na „licu mjesta“, [43].

c) Model uređaja te podaci sa uređaja

Prilikom forenzičkog istraživanja, mora se identificirati o kojem je uređaju riječ. Osim što daje forenzičaru uvid u osnovne komponente uređaja, identifikacija također omogućuje odabir odgovarajućeg alata koji je kompatibilan s identificiranim uređajem. Pod identifikacijom uređaja podrazumijeva se da se sazna proizvođač, broj modela, operator, telefonski broj koji se koristi ili se koristio u uređaju, [44].

d) Vanjska memorija

Pod dinamičnom memorijom podrazumijevaju se memorijske kartice, prenosivi tvrdi disk i slično. Većina mobilnih uređaja na današnjem tržištu ima mogućnost stavljanja memorijske kartice (*Micro SD*) u uređaj. Ako se memorijska kartica nalazi u uređaju, forenzičar ju uklanja iz uređaja te vrši ekstrakciju podataka s nje koristeći odgovarajuće alate. Ako se kartica nalazi u uređaju prilikom ekstrakcije, može doći do kontaminacije, tj. promjene podataka, [35].

Osim toga, uređaji možda imaju vanjsku memoriju na „*cloud*-u“, tj. oblaku, točnije, *iCloud* za iOS te Google račun za android uređaje. Kako bi se pristupilo tim podacima, koji su pohranjeni na mrežama davatelja usluga, prvo se treba odobriti zahtjev od strane ovlaštenih institucija. Pod vanjsku memoriju također se može podrazumijevati „*back-up*“ na računalu, stoga je potrebno napraviti pregled i osobnog računala, [35].

e) Ostali potencijalni dokazi

Prije samog prikupljanja digitalnih dokaza, mora se pretpostaviti da na uređaju postoje i drugačiji dokazi osim samo digitalnih. To uključuje otiske prstiju, DNA i slično. Prije samog prikupljanja digitalnih dokaza, moraju se prikupiti ostali dokazi kako ne bi došlo do „kontaminacije“ , [44].

- Priprema

Faza pripreme podrazumijeva određena istraživanja koja se odnose na pripremu odgovarajućih alata, kablova, hardvera i softvera radi što uspješnije ekstrakcije. Nakon što je uređaj identificiran, forenzičar može početi s traženjem opreme koja će odgovarati identificiranom uređaju. Prije nego što se krene s ekstrakcijom podataka, forenzičar mora istražiti funkcionalnost uređaja, tj. njegovu zaštitu, operativni sustav, potrebne kablovi za spajanje, itd. Takve informacije mogu se saznati na službenim web stranicama proizvođača samog uređaja. Kada se odabire alat za ekstrakciju, postoji nekoliko parametara. Neki od njih su da li organizacija/institucija/forenzičar koji vrši ekstrakciju ima potrebni alat te o kojoj se generaciji tehnologije radi. Mora se uzeti u obzir da ne postoji alat na tržištu koje je dovoljno efikasan da izvuče sve podatke s uređaja. Postoje službene stranice u koje se mogu unijeti uvjeti na koje forenzičar može naići te mu pomoći s odabirom odgovarajućeg alata. Neke od tih web stranica su http://www.phonescoop.com/ ili https://toolcatalog.nist.gov/, [44].

- Izolacija

Mobilni uređaji su spojeni na različite mreže kao što su *Bluetooth,* WLAN, mobilna mreža, itd. Zbog toga se uređaj mora izolirati kako ne bi došlo do priljeva novih podataka (poziva, poruka, itd.) što može uzrokovati kontaminaciju. Osim kontaminacije podataka, može se dogoditi da se podaci obrišu daljinskim putem ili da budu prebrisani ako uređaj nije izoliran. Izolacija uređaja također sprječava forenzičara da ne dođe do podataka do kojih ne smije doći, tj. za koje nije unaprijed definirano da su potrebni kao što su sekretarica, e-mail, itd. Sama izolacija se postiže korištenjem faraday-e vrećice, prigušivačem mreže, vađenjem SIM kartice, kontaktiranja davatelja usluge da blokira SIM karticu, stavljanjem uređaja u zrakoplovni način rada ili nekom drugom metodom elektromagnetskog blokiranja. Problem nastaje ukoliko se ukoliko uređaj stavlja u izolacijski objekt, jer rukovanje sa istim postaje iznimno teško. Osim toga, uređaj kad je izoliran, traži mrežu što može uzrokovati da se baterija brže isprazni, [44].

- Procesuiranje

Tek nakon što je uređaj izoliran, može se početi s procesuiranjem uređaja. Alati koji se koriste su definirani u prethodnim koracima. Vanjska memorija bi se trebala procesuirati odvojeno od samog uređaja, ako je istu moguće ukloniti, dok se SIM kartica ostavlja u uređaju. Poteškoće pri otklanjanju nastaju ako je uređaj kriptiran ili forenzičar nema odgovarajući alat, [45].

- Verifikacija

Nakon procesuiranja uređaja, ključno je da forenzičar izvrši verifikaciju kako bi se utvrdilo da su izvučeni podaci pouzdani. Može se dogoditi da se izvučeni podaci ne podudaraju s drugim forenzičkim metodama ili da nisu potpuni kao kod korištenja neke druge metode. Iz tog razloga, potrebna je verifikacija.

Za verifikaciju se koristi nekoliko različitih metoda kao što su [35]:

a) Usporedba - navedenom metodom uspoređuju se izvučeni podaci s podacima koji su vidljivi na sučelju samog uređaja
b) Usporedba rezultata dobivenih koristeći više od jednog alata – korištenjem različitih alata pokušava se dobiti isti „*output*“ informacija, tj. da se dobije isti rezultat
c) Korištenje „*Hash*“ funkcije – „*Hash*“ funkcija služi za verifikaciju izvučenih podataka kako bi se utvrdilo da podaci nisu promijenjeni prilikom ekstrakcije

- Dokumentiranje

Dokumentiranje pregleda uređaja bi se trebalo raditi pravovremeno, točnije, za svaki se korak istovremeno treba voditi i dokumentiranje. U većini slučajeva, postoje već unaprijed definirani obrasci koji se samo trebaju popuniti, čime se olakšava posao.

Podaci koji se nalaze u dokumentaciji obuhvaćaju [35]:

a) Datum i vrijeme kada je pregled započeo
b) Fizičko stanje uređaja
c) Slike uređaja i njegovih pojedinih komponenti
d) Status uređaja kada je isti zaprimljen (on/off)
e) Podaci o proizvođaču i modelu uređaja
f) Alati koji su korišteni prilikom pregleda
g) Podaci koji su zabilježeni prilikom pregleda

Vrlo je bitno da podaci budu jasno dokumentirati kako bi ih se lakše moglo interpretirati.

- Prezentacija

Nakon dokumentiranja, vrši se predaja dokumentacije instituciji koja je predala zahtjev za ekstrakcijom podataka. U većini slučajeva, podaci se predaju na papiru te u digitalnom obliku. Kako bi dokazi bili jasno interpretirani na sudu, isti moraju biti i dobro obrazloženi. Pod to se podrazumijeva, da kada se prezentira neki dokaz, da isti mora biti kronološki dobro sortiran, [45].

- Pohrana

Podaci koji su prezentirani se moraju pohranit na način da budu lako dostupni dok traje samo suđenje. Budući da neka suđenja mogu trajati nekoliko godina, podaci se arhiviraju u izvornom te „neizvornom“ formatu. Razlog tome jest taj da alati koji su bili korišteni u tom trenu ne budu više dostupni (istekla dozvala, zastarijevanje alata i slično), [45].

3.4. Forenzički alati

Kao što je prethodno navedeno, ekstrakcije podataka je proces prikupljanja podataka sa svrhom dobivanja dokaza koji se mogu koristiti u sudskom procesu. Prilikom ekstrakcije podataka, vrlo je bitno da se odabere odgovarajuća metoda. Osim toga, vrlo je bitno da se odabere odgovarajući forenzički alat, kako ne bi došlo do gubitka dokaza.

Razvoj mobilnih uređaja svaki dan sve više raste. To znači da se sa svakim novim uređajem izbaci neka nova komponenta koja nije kompatibilna s forenzičkim alatom. Stoga, da bi alat bio uspješan u ekstrakciji, mora se pratiti korak s razvojem. Većina alata sastoji se od terminala te njemu pripadajućih kablova za spajanje mobilnog uređaja na terminal. Prilikom ekstrakcije podataka, mogu se koristiti alati koji ne spadaju pod forenzičke alate. Funkcija takvih alata jest napraviti dijagnostiku te upravljanje uređajem. Međutim, potrebno je ograničiti upotrebu zato što „ne forenzički" alati mogu izazvati dvosmjernu komunikaciju dok su spojeni s uređajem te kontaminirati potencijalne dokaze. Odabir odgovarajućeg alata može se izvršiti na službenoj web stranici NIST (engl. *National Institute of Standards and Tehnology*): https://toolcatalog.nist.gov/, [23].

3.4.1. Ekstrakcija s Android operativnog sustava

Kao što je prikazano na slici 4 (zastupljenost operativnog sustava tokom godina), Android operativni sustav je postao najzastupljenija platforma na modernim pametnim telefonima. Iako je najzastupljeniji, operativni sustav mora biti optimiziran na različite načine za različite uređaje. Po tome, može se zaključiti da je Android operativni sustav „najraznolikiji" od ostalih prisutnih na tržištu. Android operativni sustav temelji se na *linux*-ovoj jezgri uz dodatne izmjene od strane *Google*-a koji je vlasnik operativnog sustava. Android koristi otvoreni operativni sustav što znači da je fleksibilan i dostupan različitim proizvođačima uređaja. Android koristi *Google Play Store* za skidanje aplikacija na uređaj. *Google Play* omogućava skidanje velikog broja aplikacija, što predstavlja problem zato što je relativno mali broj aplikacija kompatibilan s forenzičkim alatima. Osim toga, problem može predstavljati sigurnosna zaštita na uređaju, kao što je uzorak za otključavanje, pin, itd. Kako bi se zaobišle takve metode zaštite, potrebno je ući u „*debug mode*" ili je ekstrakciju potrebno izvršiti s JTAG metodom ekstrakcije, [46].

Jedna od mogućnosti koje se nude pod ekstrakcijom podataka jest kopiranje podataka s memorije uređaja na vanjsku memoriju, čime se izbjegava korištenje računala. Većina uređaja sa Android operativnim sustavom imaju mogućnost stavljanja dodatne memorije ili memorijske kartice. Kako bi se iščitali podaci s memorijske kartice, potrebno je vidjeti ima li uređaj ima u sebi memorijsku karticu. Zatim, potrebno je imati čitač za memorijsku karticu, bazu podataka za dokumentiranje, modul za prijavu slučaja i otvorenu arhitekturu, kako bi se mogla izvršiti komunikacija s drugim forenzičkim stanicama. Kako bi se sačuvali podaci a interne memorije uređaja, u uređaj se stavlja memorijska kartica od strane forenzičara. Na toj memorijskoj kartici se nalazi „*Efficient Generalized Forensics Framework Acquisition App*". Nakon što se stavi memorijska kartica, potrebno je pokrenuti aplikaciju kako bi se ugasili svi nepotrebni procesi u mobitelu. Nakon toga provodi se kopiranje podataka na memorijsku karticu, [47].

3.4.2. Ekstrakcija s iOS

iOS operativni sustavi su složeni i kompleksni kada je u pitanju ekstrakcija podataka. Apple je sve svoje uređaje zaštitio kriptografskim čipom koji vrši zaštitu svih podataka na uređaju. Sa svakom novom verzijom operativnog sustava, ekstrakcija podataka se otežava. Kako bi se mogla izvršiti ekstrakcija podataka, moguće je izvršiti nekoliko metoda, kao što su probijanje lozinke koristeći metodu „direktan napad“, izvršavanje „*jailbreak*-a“ na uređaju te slanje uređaja u Apple. „Direktan napad“ je metoda unosa lozinke dok se lozinka ne pogodi. Međutim, probijanje lozinke na taj način može potrajati pa se može koristiti „*jailbreak*“, [48].

Opcija „*jailbreak*“ omogućuje korisniku uređaja veće ovlasti nad istim. Razlog tome zašto se izvršava isti jest taj da su iOS uređaji iznimno ograničeni zbog sigurnosnih mehanizama koje je postavio proizvođač uređaja, Apple. Izvršavanjem navedene opcije zaobilaze se sigurnosni mehanizmi te se omogućuje širi spektar opcija, tj. korištenje aplikacija/softvera koji ne spadaju pod *Apple store*. Zbog toga, „*jailbreak*“ se može koristiti prilikom ekstrakcije podatka s uređaja kako bi se postigla kompatibilnost s istim. Osim toga, iOS uređaji ne podržavaju memorijsku karticu; to znači da se sav sadržaj pohranjuje na internu memoriju uređaja, [49].

Korištenjem fizičke metode ekstrakcije, kopira se memorija bit po bit te se mogu prikupiti dokazi koji su obrisani. Međutim, kod iOS uređaja dolazi do problema sa ekstrakcijom zato što je interna memorija uređaja podijeljena na dva dijela. Jedan dio se koristi za pohranu aplikacija i operativnog sustava, a drugi dio se koristi za pohranu korisnikovih informacija. Zatim, kada se pokuša izvršiti ekstrakcija podataka, forenzički alat mora biti instaliran na iOS uređaju, a onemogućeno je korištenje aplikacija/alata koje nisu odobrene i verificirane od Apple-a. Iz tog razloga provodi se „*jailbreak*“, [50].

3.4.3. Ekstrakcija s *Windows Phone*-a

Windows Phone je relativno nov na tržištu, dizajniran od strane *Microsoft*-a. Budući da je nedavno pušten na tržište, uređaj ima nekoliko razina zaštite. Za razliku od iOS i Android operativnih sustava, prikupljanje podataka je moguće koristeći samo JTAG, *Chip-off* i ručne metode ekstrakcije. Zbog visoke razine zaštite, logička metoda ekstrakcije nije moguća, [51].

Prikupljanje podataka može se ostvariti uz implementaciju „agenta“. „Agent“ je aplikacija koja se instalira na uređaj te uz pomoć zapovjedih kodova omogućava pristup podacima u uređaju. Aplikacija se instalira povezivanjem računala s mobilnim uređajem ili putem *bluetooth*-a, [52].

3.4.4. Ekstrakcija podataka sa SIM kartice

SIM kartica je komponenta koja spaja funkcionalnost uređaja s davateljem usluge. Drugim riječima, da nema SIM kartice, uređaj ne bi mogao obavljati svoje osnovne funkcije (pozivi, poruke, itd.). Podaci koji se mogu dobiti prilikom ekstrakcije podataka mogu značajno utjecati na ishod sudskog spora. Kako bi se izvršila ekstrakcija podataka, potrebno je izvaditi SIM karticu iz uređaja te ga staviti u čitač SIM kartice.



Slika 7: Čitač SIM kartice, [53]

Podaci koji se dobivaju su [54]:

- Podaci o korištenoj usluzi
- Lista poziva i kontakti
- Podaci o lokaciji
- Podaci o porukama

Davatelj usluge u većini slučajeva stavlja svoj logo na SIM karticu pa se isti može identificirati uz pomoć fizičkog pregleda SIM kartice. Osim toga, sa SIM kartice može se iščitati ICC-ID i IMSI. Pomoću tih podatka, može se izvršiti identifikacija pretplatnika i davatelja usluge, zato što su ti podaci jedinstveni za svaki SIM te se ne mogu mijenjati. Osim toga, može se dobiti i MSISDN (engl. *Mobile Station International Subscriber Directory Number*), ali za razliku od ICC-ID i IMSI-a, on nije jedinstven te ga korisnik može mijenjati, [55].

Na SIM kartici nalazi se imenik. U imeniku se nalaze imena i brojevi kontakata koji su pohranjeni na SIM kartici. Unatoč tome, SIM kartice imaju svoj kapacitet do kojeg mogu pohranjivati brojeve. Današnje SIM kartice imaju kapacitet do 500 kontakata. Osim toga, SIM kartica može sadržavati podatke o zadnjim pozivanim brojevima, neovisno da li se poziv uspješno uspostavio ili ne, [55].

Podaci o lokaciji mogu se dobiti na temelju spajanja SIM kartice na bazne stanice od strane davatelja usluge. Spremaju se podaci o području na kojem se korisnik nalazi. Za glasovnu komunikaciju se koristi LAI (engl. *Location Area Information*) te se isti sastoji od MCC (engl. *Mobile Country Code*) i MNC (engl. *Mobile Network Code*) područja na kojem se nalazi te identifikator bazne stanice LAC (engl. *Location Area Code*). Ako se uređaj isključi, sprema se zadnja poznata lokacija, tj. zadnji poznati LAI, [54].

Pod podacima o porukama podrazumijevaju se sadržaj SMS-a, datum i vrijeme slanja, broj na koji je SMS poslan te sam status poruke (pročitana, nepročitana, itd.). Kada se poruka obriše preko sučelja uređaja, ista je u uređaju označena kao slobodan prostor/memorija. Unatoč tome, poruka ostaje na uređaju, dok se ne prebriše s novom porukom, [54].

3.5. Prikupljanje podataka uz suradnju s operaterom/davateljem usluga

Ovlaštene institucije imaju mogućnosti dobiti pristup podacima o određenom pojedincu koji koristi usluge operatora. Te iste institucije ostvaruju pristup podacima na temelju pisanog zahtjeva. Na temelju tog pisanog zahtjeva, vrši se komunikacija između operatora i nadležnih institucija. Na tablici 1 vidi se koji se podaci mogu dobiti od operatora, a koji se podaci mogu dobiti s uređaja te se mogu uočiti koje su specifičnosti za jedan, a koje za drugi način prikupljanja podataka.

Tablica 1: Usporedba podataka koji se mogu dobiti iz uređaja i od davatelja usluge.

<table>
<tr><th>Podaci dobiveni od operatora</th><th>Podaci dobiveni sa uređaja</th></tr>
<tr><td>Podaci o lokaciji</td><td>Podaci stvoreni od strane korisnika</td></tr>
<tr><td>Povezivanje na bazne stanice tokom određenog vremena

Lokacija u određenim trenutcima

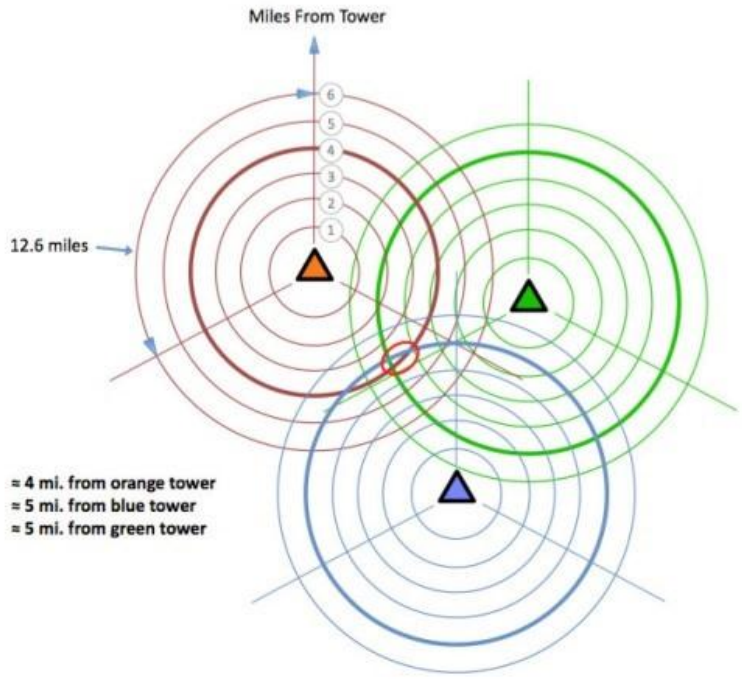
Trenutna lokacija (nepouzdano)</td><td>Fotografije
Video i audio zapisi
Datoteke različitih formata (PDF, Office Word, itd.)
Zapamćena računala na koje se pojedinac spajao</td></tr>
<tr><td>Pretplatnički podaci</td><td>Informacije o spajanju na Internet</td></tr>
<tr><td rowspan="5">Ime
Prezime
Identifikacijski broj/OIB
Prijavljena adresa
Adresa za slanje računa
Korištena usluga
Ispis transakcija (odlazni pozivi, SMS, itd.)</td><td>Računi za e-mail te društvene mreže</td></tr>
<tr><td>Aplikacije</td></tr>
<tr><td>Aplikacije koje omogućuju komunikaciju (WhatsApp, Viber, itd.)</td></tr>
<tr><td>Podaci o uređaju</td></tr>
<tr><td>Model uređaja
IMEI
Verzija softvera</td></tr>
</table>

Izvor: [56]

3.6. Triangulacija mobilnog uređaja

Triangulacija mobilnog uređaja je postupak lociranja uređaja na temelju podataka dobivenih iz baznih stanica. Dokle god je uređaj upaljen ili dok je SIM kartica aktivna i u uređaju, može se izvršiti triangulacija. Razlog tome jest to što se uređaj spaja na bazne stanice kako bi koristio uslugu. Podaci o lokaciji dobivaju se na temelju spajanja uređaja na minimalno tri bazne stanice. Bazne stanice određuju lokaciju mjerenjem vremena koje je potrebno signalu da dođe od uređaja do baznih stanica, dok je brzina prijenosa signala konstanta. Kako bi se izračunala udaljenost, potrebna su bar dva parametra, a to su vrijeme i brzina koji su potrebni da se signal vrati do odašiljača, tj. bazne stanice. Također se može uzeti u obzir da bazne stanice imaju svoj određeni domet, što dodatno olakšava lociranje. Triangulacija se izvršava uz suradnju s operatorom te, da bi se dobili takvi podaci, ovlaštene institucije moraju predati pisani zahtjev, [57].

U forenzici, triangulacija se koristi za verifikaciju alibija ili čak dokazivanja da je krivac bio na mjestu zločina. Za primjer lociranja mobilnog uređaja može se uzeti slučaj Antonije Bilić koja je bila oteta i silovana od strane Dragana Paravinje. Okrivljenika su povezali s Antonijom Bilić zato što se lokacija mobitela žrtve i okrivljenika bila poklapala na nekoliko lokacija, [58].



Slika 8: Triangulacija mobilnog uređaja na temelju spajanja na bazne stanice, [59]

4. Izazovi prilikom prikupljanja dokaza

Prilikom prikupljanja dokaza nailazi se na veliki niz prepreka. Neke od tih prepreka mogu uvelike utjecati na pouzdanost podataka dobivenih ekstrakcijom. Osim toga, podaci mogu biti „kontaminirani“, obrisani nestručnim rukovanjem ili daljinskim putem. Kako je već prethodno napomenuto, iOS operativni sustavi mogu obrisati podatke sa uređaja koristeći *iTunes* na računalu, dok Android operativni sustav može pobrisati podatke koristeći *Google*-ovu uslugu „*Find my Phone*“. Prije nego što se krene u proces ekstrakcije podataka, nužno je znati na koje izazove forenzičari mogu naići.

4.1. Izazovi uzrokovani trenutnim poteškoćama

Najčešće poteškoće na koje se nailazi su:

- Operatori i proizvođači

Prilikom preuzimanja uređaja na analizu, nužno je da se uređaj identificira. Postoji veliki broj operatora/davatelja usluga kao i samih proizvođača, što može predstaviti problem prilikom identifikacije uređaja. Razlog tome jest to što isti uređaj može biti predstavljen pod različitim nazivima od strane više operatora/davatelja usluge. Točan model uređaja nalazi se iza same baterije aparata. Međutim, uklanjanjem baterije mogu se izgubiti ključni podaci sa uređaja. Osim toga, tržište je preplavljeno s novim modelima uređaja te se uređaji mogu razlikovati po veličini, komponentama, itd., [60].

- Očuvanje podataka

Kako bi podaci ostali očuvani i „originalni“, uređaj se mora izolirati, tj. mora se spriječiti dotok novih podataka. Razlog tome jest taj da dotok novih podataka može uzrokovati brisanje starijih i promjenu već postojećih podataka na uređaju. Npr. dolazni poziv može uzrokovati mijenjanje ili brisanje liste poziva u uređaju. Osim toga, problem može nastati kada se uređaj izolira, a da isti ne ostane bez napajanja. Također, dolazi problem osjetljivosti podataka. Ako je prilikom pregleda potrebno ući u neku aplikaciju, samim pristupanjem aplikaciji mogu se kontaminirati podaci, [60].

- Punjači i USB kablovi

Nakon preuzimanja uređaja, istražitelj se mora pobrinuti da uređaj ima napajanje, tj. da se baterija ne isprazni. Razlog tome jest taj što trenutni podaci mogu biti izgubljeni nakon što se mobitel isključi. RAM memorija uređaja nije u mogućnosti održati podatke te se podaci na taj način gube. Također, problem može predstavljati ako je uređaj stariji te ima različiti priključak za punjač ili je čak moguće da isti bude oštećen, [60].

- Operativni sustavi

Jedan od većih izazova koji se mogu pojaviti jest raznolikost operativnih sustava koji su trenutno na tržištu. Različiti proizvođači uređaja za svaki model mogu izbaciti drugačiju verziju operativnog sustava. To predstavlja problem zato što ne postoji jedinstven alat za sve modele uređaja. Osim toga, s unapređenjem uređaja dolazi do povećane zaštite mobilnih uređaja koju proizvođač može postaviti na isti, [61].

- Sigurnosni mehanizmi

Uređaji imaju nekoliko sigurnosnih razina za zaštitu podataka. Razina i način zaštite zavise o proizvođaču uređaja te o operatoru. Najosnovnija razina zaštita uređaja postiže se PIN (engl. *Personal Identification Number*) i PUK (engl. *Personal Unblocking Code*) kodom. PIN/PUK kodovi su kodovi koji se dobivaju sa SIM karticom. Pojedinac ima pravo na tri pokušaja unosa PIN-a, te, ako tri puta pogriješi, javlja se PUK kod. Ukoliko forenzičar nije u mogućnosti probiti ovu razinu zaštite, PUK kod se može zatražiti od davatelja usluga, tj. davatelja SIM-a, a za dobivanje informacija o sadržaju SIM-a koristi se čitač za SIM kartice. Sljedeća razina zaštite koja može predstavljati problem je zaključavanje zaslona. Zaključavanje zaslona ima nekoliko razina zaštite, a one su PIN kod, uzorak, lozinka, itd. Forenzičar ovaj način može probiti koristeći jednu od prethodno navedenih metoda ekstrakcije. Osim toga, značajnu prepreku prilikom ekstrakcije podataka predstavlja ako je pojedinac koristio usluge u oblaku i enkripcijsku zaštitu. U tom slučaju, vrlo se teško ulazi u trag počinitelju, [62].

- Različiti formati podataka

Podaci na uređaju mogu biti pohranjeni na više lokacija na uređaju. Pod to može spadati SIM kartica, RAM memorija, „*flash*“ memorija, memorijska kartica, itd. Stoga je potrebno pregledati sve vrste memorija kako se ne bi propustila neka „ključna“ informacija. U memoriji se pohranjuju podaci raznih i jedinstvenih formata. Stoga je vrlo bitno da se zna kakvu informaciju se treba tražiti (zvuk, tekst, slika, itd.), kako bi se mogao odabrati odgovarajući alat, [61].

- Ostalo

Navedeni su najčešći izazovi na koje se može naići, međutim postoji još mnogo načina koji mogu utjecati na ishod prikupljanja podataka te će ih se navesti nekoliko. Zbog povećeg broja proizvođača na tržištu, može se dogoditi da forenzičar nema odgovarajuću opremu, pa se može dogoditi slučajno resetiranje uređaja ili vraćanje na tvorničke postavke od strane forenzičara. Maliciozni programi ili virusi na uređaju mogu nepovratno uništiti podatke. Zatim, česte su situacija u kojima osumnjičenik koristi neregistrirane *prepaid* brojeve te „*burner phone*“, [62].

Budući da je korisnik neregistriran te se SIM kartica može kupiti na bilo kojem prodajnom mjestu, postaje gotovo nemoguće pronaći osobu. S druge strane, „*burner phone*“

je jednokratan mobitel koji se koristi samo za jednu zadaću/aktivnosti, najčešće kriminalnu, te se, nakon što se ispuni ta zadaća/aktivnost, uređaj uništava te baca u smeće, [62].

4.2. Nezakonito prikupljanje dokaza

Zakonima o nezakonitom prikupljanju dokaza pokušava se ograničiti Država da prilikom prikupljanja dokaza ne postupa na nehuman način prema pojedincu. Dokazne zabrane su pravila/norme o ograničenju policijskih ovlasti, odvjetništva te samog suda. Današnji kazneni postupci nalažu da, ako su dokazi pribavljeni povredom ljudskih prava i slobode građana, isti se neće razmatrati kod donošenja presude u kaznenom postupku.

Postoje tri osnovne vrste nezakonitih dokaza [63]:

- Dokazi koji su prikupljeni kršenjem temeljnih prava i slobode građana
- Dokazi za koje je definirano zakonom da ne smiju biti iskorišteni prilikom donošenja sudske odluke
- Derivirani dokazi, točnije oni dokazi koji su prikupljeni pomoću prve dvije točke koje su navedene

Osim toga, nezakoniti dokazi ne smiju se prezentirati ni predlagati pred sudom u svrhu argumentacije tokom sudskog procesa.

Daljnji detalji će se raspraviti dalje u poglavljima.

5. Pravna regulativa

Kao što je prethodno napomenuto, znanstveni i pravni aspekt digitalne forenzike su integrirani, tj. ne mogu jedan bez drugog. Ukratko, može se reći da je najbolji dokaz beznačajan, ako je dobiven ilegalno. Prilikom ekstrakcije podataka ili bilo kakvog drugog procesa u parnici, ne smije se izvršiti povreda zakonskih odredbi, kako se prikupljeni dokazi ne bi smatrali nepravovaljanima. Niže u poglavlju obradit će se osnovne zakonske odredbe koje se moraju poštovati prilikom kaznenog postupka.

5.1. Zakon o elektroničkim komunikacijama

Zakonom o elektroničkim komunikacijama definira se korištenje telekomunikacijskih mreža i usluga, zaštita korisnikovih prava. Zatim, određuuju se izgradnja, održavanje i korištenje telekomunikacijske infrastrukture, ovlasti te obaveze sudionika na tržištu, definiranje radiofrekvencijskog spektra, sigurnost u telekomunikacijama, obavljanje inspekcijskog nadzora te osnivanje nadležnog tijela za telekomunikacijske usluge sa svrhom rješavanje sporova u telekomunikacijskim sporovima.

Ovaj se Zakon prvenstveno odnosi na pravilnike koje operatori kao davatelji usluga moraju poštovati. Za tematiku ovog završnog rada, najbitnija su dva članka Zakona, a to su članci:

- Tajnosti elektroničkih komunikacija – članak 100.
- Tajni nadzor elektroničkih komunikacijskih mreža i usluga – članak 108.

Prema članku 100. Zakona, zabranjeno je slušanje, pohrana ili bilo koji drugi oblik presretanja komunikacija između korisnika, osim u slučajevima članka 108. ili u situacijama koje su definirane posebnim zakonima.

Prema članku 108. Zakona, operatori moraju omogućiti te održavati tajni nadzor mreža i usluga. Također, operatori moraju osigurati komunikaciju s tijelom nadležnim za nadzor komunikacije u skladu sa zakonom kojim je definirana nacionalna sigurnost. Obaveza operatora prema navedenom tijelu i prema tijelima koja imaju ovlasti za tajni nadzor, mora biti u skladu sa zakonima koji se tiču nacionalne sigurnosti i kaznenog postupka. Osim toga, operatori moraju ovlaštenim tijelima omogućiti trenutnu identifikaciju korisnika usluge.

Prema navedenome, može se zaključiti da se izričito zabranjuje „praćenje“ pojedinca, sve dok drugačije nije definirano. Točnije, zabranjeno je sve dok pojedinac ne utječe na nacionalnu sigurnost ili nije sudionik u nekom kaznenom djelu. U tom se slučaju može vršiti nadzor komunikacija od strane operatora, ali samo ako je to odobreno, [64].

5.2. Zakon o zaštiti osobnih podataka

Zakonom o zaštiti osobnih podataka štite se fizičke osobe te se vrši nadzor nad prikupljanjem, obradom i korištenjem podataka. Glavna svrha Zakona je zaštita pojedinca, njegove privatnosti te zaštita osnovnih ljudskih prava. Kada se vrši ekstrakcija podataka s mobilnog uređaja, vrši se obrada osobnih podataka. Prema članku 6. Zakona, osobni podaci moraju se obrađivati pošteno i zakonito. To znači da se podaci mogu prikupljati u svrhu s kojom je pojedinac upoznat te koja je u skladu sa Zakonom. Ne smije se obrađivati više podataka nego što je to nužno. Jedna od najbitnijih stavki jest ta da, prije nego što se krene vršiti prikupljanje podataka, izvršitelj mora obavijestiti pojedinca da se podaci prikupljaju. Međutim, to se može ograničiti posebnim zakonima ako je riječ o nacionalnoj ili javnoj sigurnosti. Također, može se uključiti i istraga, otkrivanja te osude počinitelja kaznenog dijela, [65].

5.3. Zakon o kaznenom postupku

Ovaj Zakon utvrđuje pravila kojima se osigurava da nitko nedužan ne bude osuđen, a da se počinitelju kaznenog djela izrekne kazna ili druga mjera uz uvjete koje predviđa Zakon i na temelju zakonito provedenog postupka pred nadležnim sudom.

Prije donošenja pravomoćne presude okrivljenik može biti ograničen u svojoj slobodi i drugim pravima samo uz uvjete koje određuje Zakon, razmjerno težini kaznenog djela, stupnju sumnje i jačini ugrožavanja ili povrede zaštićenog dobra. Zakonom o kaznenom postupku definirano je da se sudske odluke ne mogu temeljiti na dokazima koji su pribavljeni na nezakonit način. Nakon što se utvrdi da je napravljeno kazneno djelo, započinje se s kaznenim postupkom.

Prema članku 17., kazneni postupak započinje:

- Izdavanjem naloga o provođenju istrage
- Potvrđivanjem optužnice
- Određivanjem rasprave na temelju tužbe
- Donošenjem presude o izdavanju kaznenog naloga

Prilikom rasprave, okrivljenik ima pravo na pregled dokaza koji mogu biti upotrijebljeni protiv njega. Prema članku 76., okrivljenik ima pravo na komunikaciju sa svojim braniteljem, osim ukoliko je riječ o težim kaznenim djelima: ubojstva, otmica, protudržavni terorizam, krivotvorenje novaca, itd.

Prilikom same rasprave, zapisnik vodi zapisničar. Međutim, kada se obavlja prikupljanje dokaza, zapisnik može evidentirati osoba koja obavlja radnju prikupljanja. Prilikom očevida, ako se pronađu dokazi, to se navodi u zapisniku te se priključuje istom.

Prema članku 86., kada se na nekom dokazu ne može donijeti sudska odluka, sudac koji vodi raspravu će izdvojiti taj dokaz iz zapisnika. Izdvojeni dokazi čuvaju se kod tajnika suda te su strogo odvojeni od dokaza koji se mogu upotrijebiti u procesu, [66].

Prema članku 183., svakom se može omogućiti pristup zapisniku te dokazima ukoliko postoji opravdani interes. Jedini uvjet jest taj da pojedinci koji traže pristup moraju biti dio procesa koji je u tijeku. Prikupljanje digitalnih dokaza je definirano člankom 257..

Člankom 257. je definirana pretraga računala i s njima povezanih uređaja. Zatim, definrana je pretraga drugih uređaja čija je svrha prikupljanje, pohrana i prijenos podataka te telefonska i računalna komunikacija. Na temelju pisanog zahtjeva tijela koje vrši istragu, pojedinac koji koristi ili ima pristup uređaju ili nositelju podataka te davatelj usluge/operator moraju omogućiti nesmetani pristup uređaju ili nositelju podataka. Osobe ili davatelj usluge kojima je predan zahtjev za pristupom, moraju bez odgode omogućiti pristup te poduzeti mjere kojima se sprječava uništenje ili kontaminacija podataka. Predmeti/uređaji koji mogu poslužiti kao dokaz moraju se predati na zahtjev državnog odvjetnika, istražitelja ili policije.

Člankom 263. definirano je da se podaci moraju predati državnom odvjetniku u originalnom i razumljivom obliku. Podaci koji se prikupljaju se snimaju u stvarnom vremenu te se na zahtjev se mogu čuvati najdulje šest mjeseci.

Osim toga, člankom 332. definirane su posebne dokazne radnje. Posebne dokazne radnje podrazumijevaju prikupljanje dokaza uz privremeno ograničenje ustavna prava građana. Takva odluka donosi se kada se istraga ne može provesti na drugi način. Taj način prikupljanja može se odobriti samo pisanim zahtjevom državnog odvjetnika te suca istrage. Posebne dokazne radnje mogu trajati najdulje šest mjeseci, a na zahtjev državnog odvjetnika, mogu se produljiti na još šest mjeseci. Takve se radnje najčešće koriste u težim kriminalnim djelima ili kada je riječ o nacionalnoj sigurnosti.

Digitalni dokazi za posebne dokazne radnje prikupljaju se na nekoliko načina:

- nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu,
- presretanje, prikupljanje i snimanje računalnih podataka

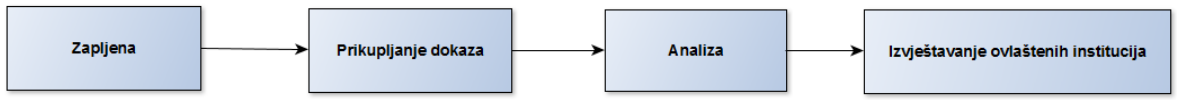
Prema članku 335., prilikom prikupljanja digitalnih dokaza, operativno-tehnički centar za nadzor telekomunikacija, uz komunikaciju sa davateljima usluge, kao i sami davatelji usluga moraju policiji omogućiti odgovarajuću tehničku pomoć, [66].

5.4. Europski protu-prijevarni ured (OLAF)

Europski protu-prijevarni ured (*European Anti-fraud Office – OLAF*) je osnovan 1999. godine od strane Europske komisije sa svrhom otkrivanja prijevara i ostalih ilegalnih aktivnosti koje bi mogle utjecati na financijski interes Europske unije. Prema regulaciji broj: 883/2013, OLAF ima ovlasti provoditi interne i eksterne istrage kako bi se spriječile prijevare. Prema uredu, definirane su procedure koje se moraju izvršavati. Ekstrakcija podataka smije se izvršavati samo uz prisustvo ovlaštenog OLAF forenzičara, dok OLAF istražitelj izvršava koordinaciju kompletne istrage. Forenzičar je dužan dokumentirati sve prikupljene dokaze, kao i okolinu u kojoj su nađeni dokazi. Ako je moguće, potrebno je izvršiti ekstrakciju podataka na „licu mjesta“ te, ako je ekstrakcija podatka izvršena, potrebno je odmah napraviti kopiju istih. Kada se forenzičar vrati u prostorije OLAF-a, dužan je odmah napraviti zapisnik aktivnosti koje su provedene prilikom prikupljanja, ekstrakcije te kopiranja podataka/dokaza. Zatim, moraju se kopirati dvije „*back-up*“ kopije dokaza te ih se mora staviti u kovertu sa jedinstvenim oznakama. Jedna se pohranjuje u arhivu OLAF-a, dok se druga kopija prosljeđuje za sudski postupak. Kopija koja ostaje u OLAF-u se učitava na interni server, dok svi mediji na kojima su se nalazili dokazi prilikom prijenosa moraju biti obrisani. Kopija koja je na serveru može se koristiti u budućim kriminalnim slučajevima, [67].

6. Tijek istrage

Metodologija u ovom procesu odnosi se na kompletan tijek istrage, dok je metodologija navedena u poglavlju 3.3.2. samo dio procesa koji se zove tijek istrage. Kao što je prethodno navedeno, procedure se moraju poštivati kako bi se olakšao i ubrzao kompletan proces. Tijekom forenzičke istrage bitno je pridržavati se koraka prikazanih na slici. Oni nisu zakonska regulativa, već su nastali na temelju dugogodišnjeg iskustva forenzičkih istražitelja, [59].



Slika 9: Tijek istrage. Izvor: [59]

6.1. Zapljena uređaja

Zapljena uređaja započinje s pisanim zahtjevom, tj. nalogom od strane državnog odvjetništva ili županijskog te kaznenog suda. Navedene institucije predaju legitimni zahtjev policiji, koja zatim provodi isti zahtjev. Kako je prethodno navedeno, prema članku 17. Zakona o kaznenom postupku, istraga započinje izdavanjem naloga o provođenju iste. Zapljena uređaja može se izvršiti sa ili bez prisustva okrivljenika, [66].

Prilikom zapljene uređaja može se izvršiti prepoznavanje, dokumentiranje te prikupljanje potencijalnih dokaza s uređaja, ako je moguće. Dokazi moraju biti očuvani kako ne bi došlo do kontaminacije ili uništenja podataka. Forenzičar prilikom zapljene uređaja mora biti upoznat s potencijalnim poteškoćama koje se mogu pojaviti te mora imati odgovarajuću opremu (USB kablovi, punjači i slično). Prve stavke koje se moraju provjeriti su memorijska kartica i SIM kartica. Razlog tome jest tošto se najviše dokaza može prikupiti sa istih, a istovremeno, mogu se najlakše sakriti ili uništiti. Osim preuzimanja uređaja, forenzičar bi trebao, ako je u mogućnosti, preuzeti i dokaze koji mogu pomoći prilikom identifikacije uređaja, kao što je kutija uređaja ili upute za rukovanje. Vrlo je bitno dokumentirati svaki postupak koji se izvrši za vrijeme rukovanja dokazima. To podrazumijeva slikanje/snimanje uređaja te njemu pripadajuće opremu, zatim snimanje okoline u kojoj je dokaz pronađen jer se svi parametri prikupljanja dokaza i okoline u kojoj je nađen uređaj uzimaju u obzir pred sudom. Nakon što se uređaj preuzme i dokumentira, potrebno ga je izolirati. Nakon što se izvrši dokumentiranje i izolacija, uređaj se pakira te se označava kao dokazni materijal, [23].

6.2. Prikupljanje dokaza

Prikupljanje dokaza može se izvršiti na „licu mjesta“ ili u laboratoriju kasnije isti dan, osim ako u nalogu nije drugačije navedeno. Pod tim se podrazumijeva da je sud donio odluku o tajnom praćenju okrivljenika te se u tom slučaju dokazi prikupljaju tokom perioda od nekoliko mjeseci. Izvršavanjem ekstrakcije podataka odmah, mogu se dobiti najpouzdanije informacije te se sprječava problem prazne baterije ili oštećenja prilikom transporta. Međutim, može se dogoditi da forenzičar nema odgovarajuću opremu pa je potrebno uređaj odnijeti u laboratorij. Kada forenzičar dođe u laboratorij, kreće se s forenzičkom analizom, [23].

6.3. Analiza

Prije nego što se krene s ekstrakcijom podataka, istražitelji ili državno odvjetništvo mogu izvršiti ispitivanje okrivljenika kako bi se olakšao postupak analize. Pod tim se podrazumijeva da isti pruži informacije ukoliko uređaj ima neku metodu zaštite, model uređaja, davatelj usluga, itd. Može se dogoditi da počinitelj bude nepoznat. Stoga je potrebno napraviti identifikaciju vlasnika uređaja. Identifikacija se može izvršiti uz pomoć podataka koji su dobiveni ekstrakcijom ili uz pomoć davatelja usluge. Sam proces forenzičke analize započinje s identifikacijom uređaja, točnije modelom uređaja, operativnim sustav te davateljem usluga. Počinitelj može pokušati prikriti navedene parametre za identifikaciju uređaja, ali postoje već prethodno spomenuti načini identifikacije. Kada se izvrši identifikacija uređaja, potrebno je odabrati odgovarajući alat. Na temelju prethodnih iskustava i na temelju naloga u kojem se nalaze podaci koji se moraju izvući, forenzičar odabire odgovarajući alat za ekstrakciju podataka, [23].

Prilikom ekstrakcije podatka, bitno je da se podaci ne obrišu ili budu kontaminirani. Nakon ekstrakcije podataka, bitno je sortirati dokaze koji se traže od onih koji su višak/nepotrebni te izvršiti verifikaciju istih. Vrlo je bitno da forenzičar dobro interpretira nalog kako se ne bi predali podaci koji nisu traženi da se ne bi dogodilo da dokazi budu odbačeni. Podaci koji se dobiju moraju se kronološki složiti sa ostalim dokazima, ukoliko isti postoje, te se vrši rekonstrukcija kompletnog događaja za koji se okrivljenik tereti od strane državnog odvjetništva. Dokaze je potrebno dokumentirati na način koji će biti jednostavan za interpretirati pred sudom, [24]

6.4. Izvještavanje ovlaštenih institucija

Izvještavanjem se podrazumijeva proces pripreme te prijave dokumentacije u kojoj se nalazi kompletan postupak procesa koji je izvršen. Pod to se podrazumijeva sažetak načina i vremena prikupljanja dokaza, koja je metoda korištena, slike uređaja i opreme, podaci o proizvođaču, status uređaja (on/off), itd. Neki forenzički alati imaju mogućnost kreiranja obrazaca koje samo treba popuniti. U tim obrascima se, osim navedenih podataka, nalaze podaci o forenzičaru, datum kada je obrazac ispunjen te kategorija samih dokaza. Dokumentaciju je potrebno predati u jednom formatu (PDF, *Microsoft Office Word*, *Power Point*, *videoplayer* itd.) koji je dostupan svima za korištenje. Nakon što se dokumentacija preda državnom odvjetništvu, ista se prezentira pred sudom te se na temelju prezentiranih dokaza donosi konačna odluka. Nakon što se donese odluka, neovisno o ishodu, dokazi se moraju pohraniti. Pohranjeni dokazi mogu se koristiti za drugi sudski slučaj, dok se za isti slučaj ne može ponovno podići optužnica, [24].

7. Zaključak

Korištenje mobilnih uređaja u kriminalnim aktivnostima povećao se proporcionalno sa samim razvojem istih. Budući da uređaji omogućavaju veliki broj funkcionalnosti, te funkcionalnosti se mogu zloupotrijebiti na veliki broj načina, pa zbog toga postoje određene metode prevencije. Međutim, mobilni uređaj može biti upotrjebljen kao alat prilikom počinjenja kriminalnog djela, što se teško može spriječiti.

Kada se izvrši kriminalno djelo, potrebno je pronaći krivca. Samu istragu provode za to ovlaštene institucije, dok je forenzičar samo sudionik u kompletnom procesu. Kako bi istraga bila uspješna, sam forenzičar mora imati iskustva i znanja za provođenje forenzičkog ispitivanja. Kao što je prethodno navedeno, tržište mobilnih uređaja je u stalom razvoju te se svaki tjedan izbaci novi model uređaja koji je jedinstven. Zbog toga, forenzičar može naići na probleme ukoliko nema odgovarajuću opremu, a čak je moguće da oprema za novi model uređaja ne postoji.

Kompletan forenzički proces je iznimno kompleksan. Razlog tome jest to što je ekstrakcija podataka s mobilnog uređaja samo jedan korak koji se obavlja u forenzičkom procesu. Pod to se podrazumijeva činjenica da se mora dokumentirati svaka aktivnost koja se obavlja prilikom rukovanja dokazom. Ukoliko je neka metoda koja je upotrijebljena prilikom prikupljanja dokaza nezakonita, taj će dokaz biti odbačen. Razlog tome jest taj što se moraju poštovati stroge procedure i zakonske odredbe jer je forenzika „isprepletena“ sa zakonskom regulativom, što znači da ne mogu ići jedna bez druge.

Korištena literatura

Stručni članci:

[1] William G.Eckert, (Godina 1992.), Intorudction to Forensic Sciences – 2nd Edition, New York: Elsevier, 1992.

[2] Leonetti, Carrie (Godina 2009.), Independent and Adequate: Maryland's State Exclusionary Rule for Illegally Obtained Evidence, University of Baltimore Law Review.

[3] Mark Pollitt, A History of Digital Forensics, Chapter 1

[4] Comprehesive Study on Cybercrime, United Nation Offfice on Drugs and Crime, Vienna, 2013. godina

[5] John Sammons, (Godina 2012.), The Basic of Digital Forensics – The Primer for Getting Started in Digital Forensics, Elsevier, Chapter 1

[10] Rick Ayers, Sam Brothers, Wayne Jansen, (Godina 2007.), NIST Special Publication 800-101 Revision 1, Guidelines on Mobile Device Forensics, National Institute of Standards and Technology

[11] Cynthia A. Murphy, Developing Process for Mobile Device Forensics

[23] Rick Ayers, Sam Brothers, Wayne Jansen, (Godina 2014.), NIST Special Publication 800-101 Revision 1, Guidelines on Mobile Device Forensics, National Institute of Standards and Technology

[24] Rick Ayers, Sam Brothers, Wayne Jansen, (Godina 2007.), NIST Special Publication 800-101 Revision 1, Guidelines on Mobile Device Forensics, National Institute of Standards and Technology

[27] Eoghan Casey and Benjamin Turnbull, 2011 Eoghan Casey. Published by Elsevier Inc, Digital Evidence on Mobile Devices

[31] Kyle D. Lutes, Richard P. Mislan, Challenges in Mobile Phone Forensics; Computer & Information Technology Purdue University

[35] Cynthia A. Murphy, Developing Process for Mobile Device Forensics

[44] Cindy Murphy, Cellular Phone Evidence Dana extraction and documentation

[47] Ahmed Rizwan, Dr. Rajiv V. Dharaskar, Dr. Vilas M. Thakare, Digital evidence extraction and documentation from mobile devices, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 1,January 2013

[54] Wayne Jansen, Rick Ayers, Forensic Software Tools for Cell Phone Subscriber Identity Modules, Conference on Digital Forensics, Security and Law, 2006

[56] Eoghan Casey, Benjamin Turnbull, Digital Evidence o Mobile Devices

[60] Kyle D. Lutes, Richard P. Mislan, Challnges in Mobile Phone Forensics, Computer & Information Technology Purdue University

[61] Dasardi Manendra Sai, Nandagiti RGK Prasad, Satissh Dekka, The Forensic Process Analysis of Mobile Device

[63] Prof. dr. sc. Davor Krapac, Nezakoniti dokazi u kaznenom postupku prema praksi europskog suda za ljudska prava

Internetske stranice:

[6] URL: http://dujs.dartmouth.edu/2013/03/computer-forensics-in-criminal-investigations/ [15.07.2017.]

[7] URL: https://www.omicsgroup.org/journals/digital-forensic-issues-in-civil-proceedings-2169-0170.1000110.pdf [15.07.2017.]

[8] URL: https://www.vecernji.hr/vijesti/teroristi-dogovarali-napad-na-pariz-putemplaystationa-1037675 [15.07.2017.]

[9] URL: http://www.fsijournal.org/article/S0379-0738(06)00383-5/fulltext?cc=y= [16.07.2017.]

[12] URL: https://www.digitaltrends.com/mobile/cdma-vs-gsm-differences-explained/ [19.07.2017.]

[13] URL: https://www.pcmag.com/article2/0,2817,2407896,00.asp [19.07.2017.]

[14] URL: http://www.computerworld.com/article/2514783/mobile-wireless/sprint-s-iden-finally-headed-for-sign-off.html [19.07.2017.]

[15] URL: http://imei-number.com/what-is-imei-number/ [19.07.2017.]

[16] URL: http://searchmicroservices.techtarget.com/definition/software [20.07.2017.]

[17] URL: http://whatis.techtarget.com/definition/operating-system-OS [20.07.2017.]

[18] Peraković ,D.: Autorizirana predavanja iz kolegija Terminalni uređaji: 9. predavanje, Fakultet prometnih znanosti, Zagreb, 2016.

URL: http://e-student.fpz.hr/Predmeti/T/Terminalni_uredaji/Materijali/09_Operativni_sustavi_terminalnih_uredjaja.pdf

[19] URL: https://www.phonearena.com/news/Cant-uninstall-an-Android-app-This-could-be-your-problem_id61301 [22.07.2017.]

[20] Peraković ,D.: Autorizirana predavanja iz kolegija Terminalni uređaji: 4. predavanje, Fakultet prometnih znanosti, Zagreb, 2015.

URL: http://e-student.fpz.hr/Predmeti/T/Terminalni_uredaji/Materijali/04_Arhitektura_terminalnih_uredjaja.pdf

[21] URL: http://www.gsmarena.com/glossary.php3?term=cpu [22.07.2017.]

[22] URL: http://www.gsmarena.com/glossary.php3?term=gpu [22.07.2017.]

[25] URL: https://www.linkedin.com/pulse/why-do-mobile-phones-need-sim-card-patrick-mutabazi [06.08.2017.]

[26] URL: https://www.elprocus.com/how-sim-card-works/ [06.08.2017.]

[28] URL: http://www.businessinsider.com.au/androids-mobile-devices-control-60-of-the-global-computing-platform-market-2013-9 [06.08.2017.]

[29] URL: https://www.digitaltrends.com/apple/smartphone-market-growing-faster-than-anticipated/ [08.08.2017]

[30] URL: https://support.apple.com/kb/PH2701?locale=en_US [08.08.2017.]

[32] URL: https://mobileforensics.files.wordpress.com/2007/03/rf-isolation.pdf [08.08.2017]

[33] URL: http://dujs.dartmouth.edu/2013/03/computer-forensics-in-criminal-investigations/ [08.08.2017.]

[34] URL: https://www.cultofmac.com/324794/cell-jamming-gives-science-teacher-an-important-legal-lesson/ [09.08.2017.]

[36] Peraković, D.: autoriziranja predavanja iz kolegija Terminalni uređaji: 12. predavanje, Fakultet prometnih znansoti, Zagreb 2017.

URL: http://e-student.fpz.hr/Predmeti/T/Terminalni_uredaji/Materijali/12_Forenzicka_analiza_terminalnih_uredjaja.pdf

[37] URL: https://www.cclgroupltd.com/mobile-device-forensics-data-acquisition-types/ [09.08.2017.]

[38] URL: https://digital-forensics.sans.org/blog/2008/09/03/hex-dumping-flash-from-a-mobile [13.08.2017.]

[39] URL: http://www.binaryintel.com/services/jtag-chip-off-forensics/jtag-forensics/ [13.08.2017.]

[40] URL: http://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/ [13.08.2017.]

[41] URL: http://proceedings.informingscience.org/InSITE2015/InSITE15p285-299Meyer1562.pdf [14.08.2017.]

[42] URL: https://www.packtpub.com/mapt/book/networking_and_servers/9781786464200/1/ch01lvl1sec11/the-mobile-phone-evidence-extraction-process [14.08.2017.]

[43] URL: https://www.packtpub.com/books/content/introduction-mobile-forensics [14.08.2017.]

[45] URL: http://resources.infosecinstitute.com/mobile-forensics-investigation-process-model/#gref [17.08.2017.]

[46] URL: https://www.lifewire.com/what-is-google-android-1616887 [17.08.2017.]

[48] URL: http://ioshacker.com/news/hackers-can-bruteforce-lockscreen-to-unlock-iphone-without-passcode [17.08.2017.]

[49] URL: http://www.techradar.com/how-to/phone-and-communications/mobile-phones/what-is-jailbreaking-1322927 [17.08.2017.]

[50] URL: http://www.csroc.org.tw/journal/JOC26-2/JOC26-2-4.pdf ili JOC26-2-4 [17.08.2017.]

[51] URL: https://www.magnetforensics.com/mobile-forensics/analyzing-windows-phone-artifacts-with-ief/ [17.08.2017.]

[52] URL: https://www.ijser.org/researchpaper/A-Novel-Method-for-Windows-Phone-Forensics.pdf [20.08.2017]

[53] URL: http://www.sirchie.com/catalog/product/view/id/2385/?___store=international_english

[55] URL: https://www.researchgate.net/publication/277814473_Forensic_Analysis_of_SIM_Cards_for_Data_Acquisition [20.08.2017]

[57] URL: https://www.iiiweb.net/forensic-services/cell-phone-tower-triangulation/ [20.08.2017]

[58] URL: http://www.jutarnji.hr/vijesti/crna-kronika/infografika-rekonstrukcija-antonija-bilic-je-pronadena-na-mjestu-koje-je-policija-vec-dva-puta-pretrazila/1367001/ [20.08.2017]

[59] URL: https://wrongfulconvictionsblog.org/2012/06/01/cell-tower-triangulation-how-it-works/ [25.08.2017.]

[62] URL: https://www.forensicmag.com/article/2013/02/6-persistent-challenges-smartphone-forensics [25.08.2017.]

[64] URL: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html [25.08.2017.]

[65] URL: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html [25.08.2017.]

[66] URL: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_152_4149.html [25.08.2017.]

[67] URL: https://ec.europa.eu/anti-fraud/investigations/digital-forensics_en [25.08.2017.]

Popis kratica

GPS	(Global Positioning System) sustav za navigaciju
IACIS	(International Association of Computer Investigative Specialists) organizacija sa svrhom educiranja na području digitalne forenzike
GSM	(Global System for Mobile Communications) tehnologija/standard koja se koristi za komunikaciju
CDMA	(Code-division multiple access) tehnologija/standard koja se koristi za komunikaciju
iDEN	(Integrated Digital Enhanced Network) tehnologija/standard koja se koristi za komunikaciju
IMEI	(International Mobile Equipment Identity) identifikacijski broj mobilnog uređaja
SoC	(System on a Chip) skup elektroničkih komponenti na jednom čipu
CPU	(Centralna procesorska jedinica) elektronička komponenta koja služi za obradu podataka
GPU	(Grafička procesorska jedinica) elektronička komponenta koja služi za obradu grafičkih podataka
RAM	(Random Access Memory) elektronička komponenta koja služi za izvršavanje programa/aplikacija
SIM	(Subscriber Identity Module) hardverska komponenta koja služi za spajanje uređaja na mrežu od davatelja usluga
ROM	(Read-only memory) elektronička komponenta koja služi za izvršavanje softvera
ICC-ID	(Integrated Circuit Card Identifier) identifikator SIM kartice
SMS	(Short Message Service) tekstualna poruka koja se šalje preko telekomunikacijske mreže
JTAG	(Joint Test Action Group) organizacija za razvoj metoda i standarda na industrijskoj razini
TAP	(Test Access Ports) portovi koji se nalaze na čipu uređaja
NIST	(National Institute of Standards and Tehnology) nacionalni institut za standarde i tehnologiju

MSISDN	(Mobile Station International Subscriber Directory Number) jedinstveni broj koji je dodijeljen korisniku usluge
LAI	(Location Area Information) identifikator područija
MCC	(Mobile Country Code) kod zemlje
MNC	(Mobile Network Code) kod mreže
LAC	(Location Area Code) kod lokacije
PIN	(Personal Identification Number) sigurnosni kod za SIM karticu
PUK	(Personal Unblocking Code) sigurnosni kod za deblokadu SIM kartice
OLAF	(The European Anti Fraud Office) Europski protu-prijevarni ured

Popis slika

Slika 1 10
Slika 2 11
Slika 3 14
Slika 4 14
Slika 5 15
Slika 6 18
Slika 7 25
Slika 8 28
Slika 9 36

Popis tablica

Tablica 1 27

Popis grafikona

Grafikon 1 4
Grafikon 2 12

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako 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 rada pod naslovom **Analiza procesa ekstrakcije podataka sa mobilnih terminalnih uređaja korištenjem forezničkih metoda u skladu sa zakonskom regulativom** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 5.9.2017

Student/ica:

Vinko Kojić
(potpis)