SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

FORENZIKA MOBILNIH UREĐAJA

Seminarski rad u okviru predmeta „Računalna forenzika“, 2017/18

Filip Lozić
0023094754

Zagreb, siječanj 2018.

Sadržaj

1. UVOD

Mobilni uređaj – pametni telefoni predstavljaju suvremeni telekomunikacijski uređaj koji je postao nezamjenjivi dio svakodnevice. Mobilni telefoni su široko prihvaćeni i lako dostupni krajnjim korisnicima koji su sve više ovisni o njima. Prosječni korisnik posjeduje po nekoliko uređaja ili korisničkih brojeva, a posebno je zanimljivo što, bez obzira na razinu tehničkog obrazovanja prema novim tehnologijama, nastoji savladati sve dostupne funkcionalnosti koje mu novi uređaj pruža. S druge strane, moderni mobilni telefoni posjeduju veliku količinu korisničkih komunikacijskih podataka (SMS poruke i poruka elektronske pošte), koriste se za bežični pristup Internetu (GPRS, EDGE, ,3G, 4G, Wi-Fi) te posjeduju razne multimedijske funkcionalnosti zahvaljujući integriranoj digitalnoj kameri, snimaču zvuka, GPS navigaciji i sl. Sve to mobilni telefon čini bogatim izvorom različitih podataka i informacija koje se mogu iskoristiti u postupku vođenja kaznenog postupka, ali i korporativne zaštite. U ovom radu je dan pregled mogućnosti mobilnih telefona kao izvora digitalnih forenzičkih dokaza i drugih informacija, kao i načina, alata i procedura prikupljanja podataka s njih.

2. OSNOVNI POJMOVI FORENZIKE MOBILNIH UREĐAJA

Forenzika mobilnih uređaja jedna je od grana digitalne forenzike, stoga je za početak potrebno definirati što je to digitalna forenzika, te što sve obuhvaća. Postoji veliki broj definicija i opisa digitalne forenzike, a ovo je jedna koja iznosi osnovne i najbitnije činjenice:

„Digitalna forenzika je znanost o identifikaciji, prikupljanju, čuvanju, skladištenju, analizi, te dokumentiranju digitalnih dokaza ili podataka koji su pohranjeni, obrađeni ili prebačeni u digitalnu formu.“

Općenito, digitalnu forenziku možemo podijeliti na pet kategorija po nazivu:

- računalna forenzika
- programska forenzika
- podatkovna forenzika
- mrežna forenzika
- forenzika mobilnih uređaja

Kao najteži dio digitalne forenzike, forenzika mobilnih uređaja se bavi prikupljanjem, obradom i pohranom digitalnih zapisa te digitalnih dokaza s mobilnih uređaja, a sve u skladu s propisima forenzičke znanosti. Također je vrlo bitno za napomenuti da se pod pojmom mobilnih uređaja ne nalaze samo mobilni telefoni, što je najčešća asocijacija. Pod pojmom mobilnih uređaja, u sklopu forenzike mobilnih uređaja, podrazumijevaju se svi uređaji koji imaju vlastitu unutarnju memoriju i sposobnost komunikacije. Između ostaloga to uključuje PDA (*eng. Personal Digital Assistant*) uređaje, GPS (*eng. Global Positioning System*) uređaje i tablete. Nastavak rada govori isključivo o mobilnim telefonima, odnosno konkretnije o pametnim telefonima.

3. DIGITALNI ZAPIS – DOKAZNI MATERIJAL

Digitalnim zapisom pametnog telefona se smatra ukupni digitalni sadržaj koji je u obliku binarnog koda zapisan na pametnom telefonu. Tu se podrazumijevaju liste poziva, SMS i MMS poruke, telefonski imenici, video i foto zapisi, povijest pretraživanja interneta, elektronska pošta, podatci s društvenih mreža, te još mnogi drugi podatci. Od cijelog digitalnog zapisa pametnog telefona digitalnim dokazom se može smatrati samo onaj dio koji je analiziran prema definiranim forenzičkim propisima te koji ima neko značenje za forenzičko ispitivanje u određenom slučaju.

3.1. Podjela digitalnih dokaza u mobilnoj forenzici

Osnovna podjela digitalnih dokaza preuzetih s pametnih telefona bazirana je na mjestu pohrane samog zapisa pa tako razlikujemo tri osnovne grupe potencijalnih digitalnih dokaza:

- Dokazi pohranjeni na SIM (*eng. Subscribe Identity Modules*) kartici
- Dokazi pohranjeni na internoj memoriji uređaja
- Dokazi pohranjeni na SD (*eng. Secure Digital*) kartici

Prilikom analize digitalnih podataka mobilnog uređaja, a u zavisnosti od tipa, moguće je više vrsta dokaza svrstati u nekoliko skupina:

- **Autorizacijski podaci –** vrsta podataka koja se koristi za identifikaciju i verifikaciju korisnika i uređaja prilikom pristupa mrežnim servisima. Razlikujemo dva osnovna podatka - IMEI (*eng. International Mobile Equipment Identity*) koji se koristi za identifikaciju mobilnog uređaja i IMSI (*eng. International Mobile Subscriber Identity*) koji nam govori o međunarodnom identifikacijskom broju korisnika.
- **Dnevnici mobilnih uređaja –** sadrži liste odlaznih, dolaznih i propuštenih poziva uključujući i vrijeme poziva, te kod uspostavljenih poziva i njihovo trajanje. Dnevnici, također, sadrže i GPS informacije, te podatke o trenutku spajanja na mrežu. Ova skupina je od velike važnosti kod forenzičkih ispitivanja jer otkriva korisnikovu lokaciju u određenom trenutku, a ponekad i kompletnu rekonstrukciju korisnikovog kretanja.

- **Kontakti –** osim kontakt brojeva, ova kategorija može sadržavati slike, fizičke adrese, e-mail adrese i mnoge druge podatke.
- **Tekstualne poruke -** sadrži podatke vrlo bitne za forenzičku analizu. Kao i kod liste poziva, koristan podatak je vrijeme nastajanja poruke. Preko tekstualnih poruka je tako često moguće rekonstruirati slijed događaja, uključujući i vremensku varijablu.
- **Kalendar –** kalendari često sadrže informacije o korisnikovim obvezama, kretnjama, različite napomene, a ponekad i kontakte. Kalendari često imaju i funkcije poput praćenja izvršavanja zakazanih obveza, te funkciju podsjetnika.
- **Elektronska pošta –** također jedan od bitnih izvora podataka, uz samu korisnikovu komunikaciju, može često sadržavati i različite popratne dokumente.

3.2. Principi digitalnih dokaza

Prema Vodiču dobre prakse o digitalnim dokazima temeljenim na računalnoj tehnologiji, a izdanom od strane ACPO (*eng. UK Association of Chief Police Officers*), postoje četiri principa digitalnih dokaza kojih se treba pridržavati:

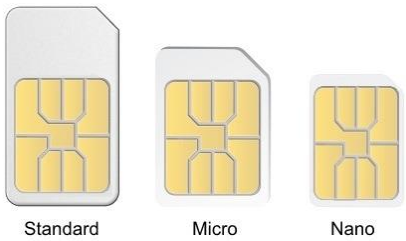
- **Princip 1 –** Agencija za provedbu forenzičkih ispitivanja niti jednom svojom akcijom ili postupkom ne smije utjecati na promjenu podataka prikupljenih s računala ili drugih medija koji mogu biti korišteni u sudskim postupcima.
- **Princip 2 –** Ukoliko postoje specifične okolnosti u kojima je potrebno izvršiti pristup originalnim podacima. To može izvršiti samo kompetentna osoba koja može obrazložiti provedene akcije nad dokazima.
- **Princip 3 –** Sve napravljene analize i ispitivanja nad digitalnim dokazima moraju biti zabilježeni, a rezultati i postupci pravilno dokumentirani. Svako ponovno provođenje istih ispitivanja ili analiza od strane treće osobe mora donijeti isti rezultat.
- **Princip 4 –** Svaki zasebni slučaj ima osobu zaduženu za njenu provedbu. Zadatak te osobe je sigurnost digitalnih dokaza, te postupanje s njima u skladu sa zakonom i navedenim principima.

4. OSNOVNI POJMOVI MOBILNIH UREĐAJA I KOMUNIKACIJA

Današnji pametni telefoni sastoje se od dva elementarna dijela: **mobilnog uređaja** (eng. *mobile equipment*) i **SIM-a** (*eng. Subscriber Identity Modules*). Mobilni uređaj je terminal koji krajnjem korisniku omogućava komunikaciju unutar mobilne mreže. U zavisnosti od modela, može sadržavati informacije poput telefonskog imenika, fotografija, audio/video sadržaja, poruka i raznih drugih multimedijskih sadržaja. Suvremeni modeli telefona sadrže velike količine memorije i time imaju mogućnost čuvanja velike količine podataka. Za uspostavu i pristup mobilnoj GSM mreži, nužno je imati SIM karticu. Ona ima sličan sadržaj kao mobilni uređaj, sadrži jedinstvenu informaciju o korisniku, kodirane identifikacijske podatke za mrežu, PIN (*eng. personal identification number*) i ostale podatke poput telefonskog imenika, poruka itd.

4.1. SIM

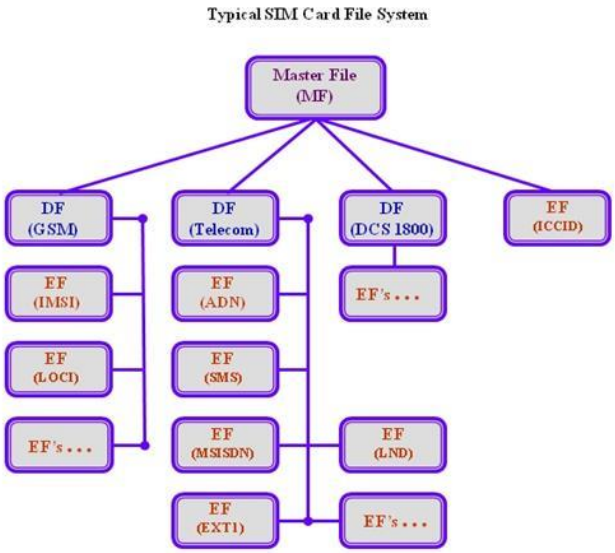
SIM kartica (*Slika 4.1.*) je vrsta *smart* kartice koja ima mikroprocesor i memoriju (najčešće 16KB i 4 MB) tipa EEPROM (*eng. Electrically Erasable Programmable Read-Only Memory*). U svojoj strukturi posjeduje i radnu memoriju (RAM) koja se koristi prilikom izvršenja reprogramiranja memorije s operativnim sistemom i algoritmima za autorizaciju korisnika i enkripciju podataka. Glavnu ulogu ima mikroprocesor koji omogućava rad i sigurnost podataka. Podaci su zaštićeni s nekoliko sigurnosnih razina koje omogućavaju kontrolu pristupa: slobodan pristup, pristup s PIN, pristup s PIN2, administracijski i zatvoreni dio.



Slika 4.1. Izgled i vrsta SIM kartica

File system SIM kartice (*Slika 4.2.*) je organiziran hijerarhijski na osnovu GSM 11.11. standarda. Sastoji se od tri dijela: glavnog root *master fila* (MF), *file system-a* i *Dedicated file-a* (DF). SIM kartice imaju analogiju kao hijerarhija file-ova na hard disku te posjeduju autorizacijske razine

za upis, čitanje, brisanje i izmjenu podatka. Velik dio podataka može se čitati bez korištenja PIN koda.



Slika 4.2. Struktura SIM kartice

SIM kartica nudi nam nekoliko važnih informacija koje mogu biti od velike važnosti prilikom forenzičke analize.

SIM sadrži informacije o:

- **ICCID** (*eng. Integrated Circuit Card Identifier*) - međunarodni identifikator mobilnog pretplatnika :
    - sadrži tri znamenke pozivnog broja zemlje, zatim MNC (01 za HT, 10 za VIP i 02 za TELE2) i serijski broj.
- **MSISDN** (eng. *Mobile Subscriber Integrated Services for Digital Network Number*) - međunarodni pretplatnički broj
- **IMSI** (*eng. International Mobile Subscriber Identity*) - jedinstven identifikator SIM kartice:
    - peteroznamenkasti broj koji se sastoji od MCC (*eng. mobile country code*) tri znamenke (219 za Hrvatsku), MNC (*eng. mobile network code*) i MSIN (*eng. mobile subscriber identity number*) gdje spadaju preostale znamenke.
- **SPN** (*eng. Service Provider Name*) - naziv mobilnog operatora

4.2. Mobilni uređaj

Mobilni telefon se poput računala sastoji od integriranih hardverskih komponenti (SIM modula, kamere, zvučnika, display-a itd.) te softverskog dijela – operacijskog sustava. Unutar samog uređaja moguće je pronaći sljedeće informacije:

- **ESN** (*eng. Electronic Serial Number*)
  - jedinstveni broj koji označava svaki uređaj.
- **MSISDN** (*Mobile Subscriber Integrated Services Digital Network Number* **)**
  - koristi za pristup korisničkim podacima unutar HLRa.
- **IMEI** (*eng. International Mobile Equipment Identifier*)
  - jedinstveni generirani petnaesteroznamenkasti broj koji je dodijeljen svakom mobilnom uređaju. Koristi se za identifikaciju u GSM, UMTS i LTE mrežama (*Slika 4.3.*).

*Slika 4.3. Prikaz IMEI broja korištenjem koda *#06#*

5. PROCEDURA PROVOĐENJA FORENZIČKE ISTRAGE

Prvi korak prilikom pronalaska uređaja na terenu, koji nosi moguće potencijalne dokaze važne za slučaj, je odraditi klasičnu forenziku u kojoj se pronalaze biološki dokazi poput otisaka prsta, DNK, itd. Tijekom cijelog procesa svaka promjena na uređaju treba se pomno bilježiti i dokumentirati, te je poželjno minimizirati diranje ekrana kao ne bi došlo do promjene podataka na samom uređaju. Potrebno je analizirati mobilni uređaj i SIM karticu, te napraviti analizu mobilne mreže i tipa podataka. Najvažniji korak prije samog ispitivanja je izolacija uređaja i zaštita od mogućih napada.

5.1. Izoliranje mobilnog uređaja

Nakon fizičke obrade treba provjeriti je li uređaj upaljen. Ako nije upaljen, treba provjeriti postoji li SD kartica. U slučaju da postoji, treba napraviti sliku podataka na njoj te napraviti identičnu kopiju kartice koja se potom vrati u mobitel. Prva stvar koju trebamo napraviti, ukoliko dobijemo ili pronađemo uključeni mobitel ili vršimo paljenje telefona, je mrežna izolacija. U nastavku je dano nekoliko načina mrežne izolacije od kojih svaka ima neke dobre i loše strane:

- **Način rada u zrakoplovu** (*eng. Airplane Mode*) – u većini slučajeva najbolji izbor jer pravi izolaciju od svih mreža kao što su mobilne, Wi-Fi, Bluetooth, ali potencijalni minus mu je što mijenja stanje uređaja. Zbog toga se sve treba dobro dokumentirati.
- **Vađenje SIM kartice** - mobilni uređaj se izolira od mobilne mreže, međutim to ne utječe na Wi-Fi i Bluetooth mreže. Kod starijih uređaja dodatni minus je to što se za vađenje SIM kartice treba izvaditi baterija čime dolazi do gašenje mobitela, gubljenje podataka iz RAM-a, moguća aktivacija šifriranja i/ili zaključavanja zaslona uređaja (PIN, password) ili čak i pokretanje brisanja čitave memorije.
- **Zahtjev mobilnom operateru da onemogući SIM karticu uređaja** – postiže se samo jedan aspekt mrežne izolacije kao i vađenjem SIM-a.
- **Faradayeva zaštita** – vrećice, kutije, šatori i sobe. Omogućava izolaciju od svih mreža, međutim smanjuje trajanje baterije zato što se uređaj konstantno pokušava spojiti na mreže. Zbog toga ga je potrebno što prije priključiti na napajanje.

- **Isključivanje uređaja** - kao zadnje rješenje koje je definitivno najučinkovitije u mrežnoj izolaciji, ali kao što je rečeno mijenja stanje uređaja.

Treba se pretražiti cijelo mjesto istrage i prikupiti sve predmete koji su blisko vezani s mobilnim uređajem poput kablova, punjača, memorijskih kartica, SIM kartica, baterija, upute za upotrebu itd.

Nakon obavljene terenske analize, izolirani uređaj potrebno je dopremiti u istražni laboratorij kako bi se provele sljedeće procedure u istrazi:

- Identificirati proizvođača i model mobilnog uređaja
- Forenziku mobilne mreže
- Forenziku SIM kartice
- Akvizicija podataka sa mobilnih uređaja

Istraga mobilnih uređaja nije nimalo lagan proces. Dok se kod računalne forenzike primjenjuju poznate i definirane procedure za sve uređaje, kod mobilnih telefona, koji se međusobno razlikuju od modela do modela, jednom uspješno odrađena procedura ne osigurava 100% mogućnost primjene u nekom drugom slučaju.

5.2. Forenzika mobilne mreže

Prvi korak u forenzičkoj analizi uređaja je odrediti koji tip mobilne mreže telefon koristi. Danas su najrasprostranjenije sljedeće mreže:

- **CDMA** (*eng. Code Division Multiple Access*): Ne posjeduje SIM modul – Svi podaci nalaze se i spremaju se na mobilni uređaj. To su uređaji sa SAD tržišta.
- **GSM** (*eng. Global System for Mobile Communication*): Mreže koriste SIM module kao odvojene komponente dizajnirane da budu prenosive sa jednog telefona na drugi - koriste se u Europi i nekim istočnim zemljama.
- **IDEN** (*eng. Integrated Digital Enhanced Network*): Napredne SIM kartice – uSIM.

Vrsta mobilne mreže koja se koristi u mobilnom uređaju direktno utječe na pristup koji se koristi prilikom daljnje analize mobilnog telefona. Ukoliko se radi o GSM ili IDEN uređajima, sljedeći korak je napraviti forenziku SIM kartice.

5.3. Forenzika SIM kartice

SIM omogućava korisniku prebacivanje podataka kao što su imenik, poruke između različitih mobilnih telefona. Korisnik može svjesno mijenjati uređaj, ali se i dalje uz pomoć gore navedenih informacija može u svakom trenutku locirati. Najsigurniji način pristupa mobilnom telefonu je kloniranje SIM kartica korištenjem forenzičkih alata. SIM kartica zaštićena je PIN brojem, čiji je zadatak ne samo zaštita podataka na kartici već i na samom uređaju. Obrisani podaci sa SIM kartice mogu se vratiti uz pomoć softverskih alata. Taj postupak nam je dostupan jer podatak obrisan iz memorije bilo to na SIM kartici ili uređaju nakon operacije brisanja ne nestaje, već je označen kao slobodan prostor i čeka da se na njegovo mjesto upiše novi podatak. Za to vrijeme njegov sadržaj je i dalje prisutan i može se pročitati.

5.4. Prikupljanje podataka sa mobilnih uređaja

Forenzička ekstrakcija i izvlačenje podataka s mobilnih uređaja je jedan od najzahtjevnijih postupaka forenzičke istrage. Da bi se ona mogla pravilno izvesti, potrebno je znati kako je izvedena memorija na tom uređaju kako bi znali gdje tražiti dokaze. Stoga razlikujemo dvije vrste memorije: promjenjivu (RAM) i nepromjenjivu NAND (eMMC i SD-card) memoriju.

RAM i eMMC memorija su napravljeni zajedno na jednom čipu što uvelike komplicira forenziku tih uređaja. Te memorije nije moguće jednostavno izvaditi i spojiti na blokator pisanja i prepisati. RAM memorija služi za privremeno učitavanja, izvršavanje i manipuliranje ključnim dijelovima operacijskog sustava, aplikacija i podataka i ona se briše nakon gašenja uređaja. U njoj se mogu naći jako važni podatci kao što su lozinke, korisnička imena, ključevi za kriptiranje, podatci aplikacija kao što je primjerice broj računa. NAND memorija ostaje zapisana i nakon gašenja i ponovnog pokretanja uređaja. Na ovom elementu mobilnog telefona smješten je operativni sistem (OS), a često i softver za rješavanje problema koji se koristi za dijagnostiku i upravljanje uređaja.

Identifikacija modela mobilnog telefona provodi se pretragom proizvođača, serijskog broja uređaja koji se obično nalaze ispod baterije, sinkronizacijskim softverom ili kodovima proizvođača. Time se dolazi do informacija kao što su: proizvođač telefona, model, kod zemlje u kojoj je proizveden itd. Nakon utvrđivanja tipa mobilnog telefona, traži se lista

karakteristika koje daje proizvođač, pa se na temelju te liste izdvoje mjesta gdje je moguće pronaći određene dokazne materijale.

Pregledom specifikacija dobija se uvid u:

- Metode bežičnog spajanja: bluetooth, WiFi ili IR tehnologija
- Pristup Internetu: Wifi, GSPR, 3G,4G
- PIM (eng. Personal information manage): sadrži kalendar, imenik, kao i softver za pregled raznih tipova dokumenata
- Poruke: ima li telefon mogućnost slanja SMS poruke, multimedijalne poruke,Email-a
- Operativni sistem i aplikacije: vrsta operativnog sistema i polaznih aplikacija
- Spajanje: vrsta kablova potrebnih za spajanje s računalom

Ukoliko na uređaju tražimo određene artefakte, postoje alati koji na jednostavan način dolaze do traženih podataka na osnovu tipa, veličine i datuma kreiranja. Ako se radi analiza operacijskog sustava uređaja, uglavnom je potrebno uključiti opciju za debagiranje na uređaju i omogućiti administratorski pristup (*eng. root*).

Tablica 1. Lokacije pohrane za Android uređaje

Tip podatka	**Lokacija**
Računi	/root/system/accounts.db
Povijest pretraživanja	/root/data/com.android.browser/databases/browser.db
Kontakti	/root/data/com.android.providers.contacts/databases/contacts2.db
E-pošta	/root/data/com.android.email/databases/EmailProvider.db
SMS/MMS	/root/data/com.android.providers.telephony/databses/mmssms.db
Kalendar	/root/data/com.android.providers.calendar/databases/calendars.db

5.4.1. Datotečni sustavi

Operacijski sustavi podržavaju i korist više datotečnih sustava. Njihov popis se može naći u datoteci /proc/filesystems. Neki od najznačajnijih datotečnih sustava su :

- Rootfs – služi kao točka vezivanja za korijenski datotečni sustav (/)
- Tmpfs – datotečni sustav koji sprema podatke u virtualnu memoriju(/dev, /mnt/asec, /app-cache, /mnt/sdcard/.android_secure)
- Cgroup – je datotečni sustav koji pruža mogućnost pristupanju i definiranju različitih parametara jezgre [9] (/dev/cpuctl/acct)
- Proc – sadrži informacije o jezgri operacijskog sustava, procesima i konfiguraciji sustava (/proc)
- Sysfs – izvozi informacije o uređajima i upravljačkim programima iz modela jezgre operacijskog sustava prema korisničkom prostoru [10] (/sys)
- Devpts – koristi se za virtualne terminal sjednice (/dev/pts)
- Ext3 i ext4– standardni Linux datotečni sustavi (/cache, /system, /data/data)
- Yaffs2 - upravljanje lošim blokovima (/proc/yaffs)
- Vfat i fat32 – koriste se na SD-kartici i eMMC-u zbog kompatibilnosti s Windowsima koji su najrašireniji operacijski sustav (/mnt/sdcard, /secure/aasec, /mnt/emmc)

5.5. Ekstrakcija podataka

Postoji više tehnika kojima se mogu pribaviti informacije s mobilnih uređaja. U nastavku su objašnjene tehnike ručne, logičke i fizičke ekstrakcije podataka.

5.5.1. Ručna ekstrakcija podataka

Ručna ekstrakcija obuhvaća ručno pregledavanje podataka na mobitelu uz interakciju s ekranom i tipkama te se uglavnom koristi uz neku drugu tehniku. Sva interakcija bi trebala biti nekako zabilježena, primjerice snimljena digitalnom kamerom. Tijekom ručne ekstrakcije neizbježno se mijenja stanje uređaja, a podaci mogu biti obrisani i prepisani, te je

preporučljivo minimizirati upotrebljavanje ove metode. S njom se ne mogu pregledati obrisani podaci, a dodatne poteškoće nastaju ako je mobitel na nepoznatom jeziku.

5.5.2. Logička ekstrakcija podataka

Logička ekstrakcija podrazumijeva izvlačenje podataka s uređaja povezanoga s forenzičkom postajom (*eng. forensic workstation*). Forenzička postaja je sklopovlje, posebni uređaj ili primjerice stolno računalo, koje je pripremljeno za izvođenje digitalne forenzike svih digitalnih uređaja ili samo jednog dijela. Logičkom ekstrakcija dobivamo korisničke podatke koje su vidljive pregledavanjem SD kartice u pregledniku. Dobivaju se uglavnom neizbrisani, tj. alocirani podaci s mobitela i to je postignuto pristupanjem datotečnom sustavu. Neki izbrisani podaci se mogu pronaći u SQLite bazama podataka. U većini slučajeva ova je tehnika dovoljna za pronalaženje potrebnih informacija. Prednost u odnosu na fizičku akviziciju je to što su logičke tehnike puno brže, a nedostatak je što se njima dobiva malo ili ništa izbrisanih podataka. Za logičke tehnike, potrebno je omogućiti opcija traženja pogrešaka putem USB sučelja (*eng. USB debugging*), a administratorski (*eng. root*) pristup nije nužan. Bez administratorskog pristupa se ne može pristupiti nekim dijelovima memorije, npr. /data direktoriju, dok administratorski pristup omogućuje pristup svim podacima.

Pod logičku ekstrakcija spada i analiza sigurnosne kopije (*eng. backup*) mobitela. To podrazumijeva analizu postojeće kopije ili nove sigurnosne kopije preko aplikacija koje su isporučene direktno s mobitelom ili se instaliraju s Google Play trgovine.

5.5.3. Fizička ekstrakcija podataka

Fizičkom ekstrakcijom se podrazumijeva bit-po-bit kopija memorije zaobilaženjem datotečnog sustava. Prednost ovih tehnika je što se kopira ne samo alocirani, nego i nealocirani prostor memorije, tj. uz postojeće podatke kopiraju se i oni izbrisani i odbačeni. Također, pod fizičkim ekstrakcijama podrazumijevamo JTAG (*eng. Join Test Action Group*) i chip-off metodu. One ne zahtijevaju ni administratorski pristup ni uključenu opciju traženja pogrešaka putem USB sučelja, čime istodobno rješavamo i problem uređaja sa zaključanim zaslonom ili SIM karticom.

JTAG je ne-destruktivna metoda izvlačenja svih podataka iz uređaja kad tradicionalna forenzika zakaže. JTAG se koristi kada je uređaj zaključan lozinkom ili uzorkom, utor za prijenos podataka nedostupan ili čak kada je uređaj fizički oštećen ili djelomično uništen. Ova

specijalizirana usluga je pristupačna i prikladna za uporabu za razne osobe, uključujući policiju, odvjetnike, fizičke osobe i institucije.

Chip-off forenzika - ili forenzičko razdvajanje je učinkovito ali destruktivno i obično je posljednja opcija kada je u pitanju izvlačenje podataka iz mobitela. Ova metoda uključuje posebni proces i opremu kako bi se razdvojio memorijski čip i izvukli podaci za analizu. Konačni rezultat je taj da je uređaj uništen, ali su podaci sačuvani u forenzičkom smislu.

5.6. Alati za forenziku mobilnih uređaja

Prethodno navedene specifičnosti mobilnih telefona uvelike utječu na razvoj alata za forenziku mobilnih uređaja. Takvi zahtjevi doveli su do razvoja širokog spektra alata. Veći dio njih je namijenjen za komercijalnu upotrebu i najčešće zahtjeva osobu osposobljenu za rad dok je drugi dio alata otvorenog koda te je prilagođen manje iskusnim korisnicima. Postoje zahtjevi koji su postavljeni pred sve alate koji se koriste u forenzici mobilnih uređaja, bez obzira radi li se o komercijalnim alatima ili ne, te za koji je operacijski sustav alat namijenjen, a to su:

„Alat mora funkcionirati na način da se promjene izvornih podataka svedu na minimum. Pomoću alata se mora moći povući što veća količina podataka pohranjenih na mobilnom uređaju. Funkcioniranje alata mora biti izvedeno na način da se interakcija čovjeka s mobilnim uređajem svede na minimum“.

Na tržištu se trenutno nalazi veliki broj različitih komercijalnih alata, a u nastavku su nabrojani samo neki:

- iPhone Analyzer – ovaj alat podržava razne iOS 2.x - iOS 7 uređaje. Moguće ga je koristiti na raznim platformama (Linux, Windows, Mac).
- viaForensics' Forensics – je grupacija koja nudi nekoliko alata za ovu namjenu, od koji su neki za komercijalnu upotrebu, a drugi otvorenog koda. Jedan od poznatijih alata im je viaExtract, a namijenjen je pametnim telefonima zasnovanima na Android platformi.
- Magnet forensic – je komercijalni alat, ali prilagođen krajnjem korisniku te je vrlo jednostavan za osnovno korištenje.

ZAKLJUČAK

Digitalna forenzika mobilnih uređaja još uvijek je mlada grana forenzičke struke koja ima vrlo važnu ulogu u razvoju sigurnosti. Podloga ovakvom načinu razmišljanja uglavnom proizlazi iz kontinuiranog razvoja mobilne industrije koja pripada najbrže rastućoj industriji. Upravo ta dinamika razvoja te nepredvidivost kretanja mobilne industrije pred digitalnu forenziku mobilnih uređaja postavlja najveće izazove.

Sve širi spektar funkcionalnosti i mogućnosti koje pametni telefoni pružaju svojim korisnicima čini ih sve poželjnijim uređajima za organizaciju, praćenje i unaprjeđenje kako poslovnih, tako i privatnih obveza. Uz sve navedeno pametni telefoni postaju sve češći alati ili pomagala za provedbu digitalne manipulacije podacima. Upravo te činjenice daju još veću važnost digitalnoj forenzici mobilnih uređaja, alatima za njenu provedbu te ljudima koji se njome bave.

Prosječnom korisniku mobilnog uređaja je moguće pomoću jednostavnog, neprofesionalnog alata za provedbu digitalne forenzike mobilnih uređaja vrlo lako doći do poruka, poziva ili slika i ostalih dokumenata koji su ranije pobrisani s uređaja.

LITERATURA

1. Jovanović, *Forenzika mobilnih uređaja*, Diplomski rad, Sveučilište Niš, 2014.
2. Prezetacija "*Forenzika mobilnih uređaja*", Digitalna forenzika, Sveučilište Niš, 2014
3. Računalna forenzika, CARnet, 2010
4. Rizwan, A. i Raiv, V.D. Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcment perspective. *Emerging Technologies in E-Government* (2009).
5. Iosif I. Androulidakis,"Mobile Phone Security and Forensics", London, 2012.
6. Andrew Hoog, Android forensics, Sjedinjene Američke Države: Syngress, 2011
7. The Future of Mobile Forensics: November 2015 Follow-Up https://articles.forensicfocus.com/2015/11/04/the-future-of-mobile-forensics-november-2015-follow-up
8. Internet, Forenzika mobilnih uređaja, http://detektiv-mreza.hr/hr/specijalnost/forenzika-mobilnih-uredaja-1