Forenzika mobilnih uređaja mogućnosti i izazovi

iOS & Android

Tanja Kaurin
Katedra za bezbednost i kriminalistiku
Fakultet za pravne i poslovne studije dr Lazar Vrkatić
Novi Sad, Srbija
tanja.kaurin@useens.net

Sažetak—**Digitalni uređaji su postali sastavni deo našeg života. Intenzivna upotreba u svakoj sferi kao i njihova sposobnost memorisanja aktivnosti sa ekstremnim detaljima, pretvara ih u digitalne baze podataka ponašanja njihovih korisnika. U širokoj paleti digitalnih uređaja definitivno se izdvajaju mobilni telefoni, svakodnevni pratioci vlasnika, čuvari vitalnih podataka njihovih života, kako njihove realnosti tako i skrivenih želja, sklonosti i planova. Ogromne mogućnosti obrade podataka na osnovu kojih je moguće formirati profil korisnika, dokazati lokacije i izvršene aktivnosti te potencijalno pretpostaviti one koje će se tek dogoditi stvaljaju ih u sam vrh uređaja atraktivnih za digitalnu forenziku. Iako trenutna ponuda alata za mobilnu forenziku nudi zadivljujući broj podataka koje je moguće sakupiti treba biti svestan realnih mogućnosti, eventualnih prepreka i izazova.**

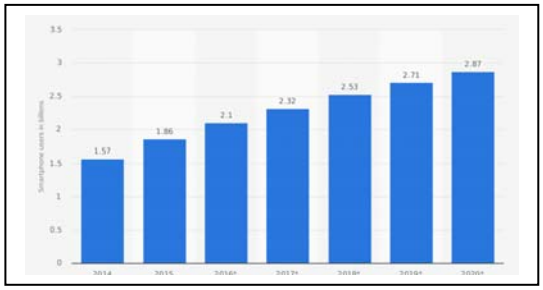
Cilj rada je da ukaže na mnogobrojne postojeće i vrtoglavo rastuće izazove u ovoj oblasti zbog visokog nivoa zaštite podataka na kome rade proizvođači, kao i da ukaže na trendove i tendecije razvoja forenzike mobilnih uređaja analizom postojećeg stanja i predstavljanjem mogućnosti ekstrakcije podataka na dve najzastupljenije mobilne platforme na trzistu (iOS i Android).

Ključne riječi – forenzika mobilnih uređaja; ekstrakcija podataka; Cellebrite UFED;

I. UVOD

Mobilna tehnologija je prešla dugačak put od Drugog svetskog rata kada su vojnici nosili telefon težak oko 11 kg. sa dometom od 8 km. do današnjih telefona od stotinak grama [1]. Zbog nesumnjivih brojnih prednosti, mobilni uređaji su godinama unazad u epicentru ubrzanog tehnološkog razvoja. Popularnost im svakodnevno raste a sa njom i pospešivanje razvoja pratećih tehnologija: Internet stvari, Cloud Computing i Big Data. Mobilni uređaj kao alat koji spaja skoro svaku aktivnost, privatnu i poslovnu, definitivno se smatra neophodnim za većinu stanovnika na planeti.

Brojke su uvek jasan pokazatelj trenda te su na Sl. 1 predstavljeni podaci objavljeni na portalu Statista sa pregledom broja korisnika smart telefona (u milijardama) širom sveta od 2014. godine kao i predviđanje rasta do 2020. [2]. Očigledan je godišnji konstantan rast, do procenjenih oko tri milijarde uređaja 2020. godine. Prema podacima kompanije Gartner globalna prodaja pametnih telefona u prvom tromesečju 2017. godine je iznosila 380 miliona jedinica.



Slika 1. Broj korisnika smart telefona širom sveta 2014. - 2020.

Navedena brojka predstavlja porast od 9,1 posto u odnosu na prvi kvartal 2016. godine [3]. Ukupna isporuka digitalnih uređaja (računari, tableti i mobilni telefoni) iznosila je 2,28 milijardi jedinica u 2017. godini dok se za 2018. očekuje povećanje od 2,1 te dostizanje cifre od 2,32 milijarde jedinica [4].

Sveprisutnost mobilnih uređaja povećava značaj digitalne forenzike istih jer omogućava pribavljanje ličnih podataka korisnika koje je teško ili nemoguće obezbediti na neki drugi način. Sa porastom mobilnih uređaja raste svest o bezbednosti podataka na njima, pre svega od strane proizvođača ali i od strane samih korisnika. Proizvođači mobilnih uređaja polako uvode enkripciju što značajno otežava proces digitalne forenzike. Pred forenzičare se stavljaju dodatni izazovi te se može reći da zlatno doba digitalne forenzike prestaje, sve je manje nezaštićenih uređaja i aplikacija, samim tim sve manje alata koji će omogućiti sakupljanje podataka i osobama bez tehničkog znanja, kao što je to do skoro bio slučaj. Pored toga, podaci i dalje ostaju ranjivi te je prilikom sakupljanja neophodno strogo poštovati pravila digitalne forenzike te primenjivati adekvatne metode i tehnike.

U radu su predstavljeni izazovi mobilne forenzike kao i trenutne mogućnosti. Uvodom u forenziku mobilnih uređaja kroz poglavlje II navedene su osnovne faze forenzike mobilnih uređaja i objašnjene metode ekstrakcije, prednosti i mane kao i parametri koji utiču na izbor metode. U poglavlju III skrenuta je pažnja na neke od ključnih izazova a u IV sa forenzičkog aspekta objašnjena dva najzastupljenija operativna sistema (iOS&Android). Poglavlje V obiluje detaljnim podacima ekstrakcije, u tabelarnom prikazu, kako bi na što jednostavniji način bile predstavljene trenutne mogućnosti mobilne

forenzike. Za ekstrakciju su korišćeni podaci izraelske kompanije Cellebrite, svetskog lidera u oblasti forenzike mobilnih uređaja.

II. FORENZIKA MOBILNIH UREĐAJA

Forenzika mobilnih uređaja se smatra ogrankom digitalne forenzike koja podrazumeva sakupljanje i povraćaj podataka, potencijalnih digitalnih dokaza, sa mobilnog uređaja u skladu sa pravilima forenzičke nauke [5]. Iako termin "mobilni uređaj" obuhvata širok spektar uređaja koji se kreću od mobilnih telefona, pametnih telefona, tableta i GPS uređaja do nosivih (*wearables)* i PDA, zbog brojčane nadmoći mobilnih telefonskih uređaja najčešće se zapravo govori o forenzici mobilnih telefona. Ipak ono što svi navedeni uređaji imaju zajedničko je činjenica da mogu sadržati puno specifičnih informacija vezanih za korisnika.

Osnovni princip digitalne forenzike uopšte te i forenzike mobilnih uređaja je sačuvati originalni podatak od promena. Upravo ovaj princip je izuzetno teško ispuniti kod mobilnih uređaja jer su podaci krhke prirode i lako mogu biti modifikovani, uništeni ili izgubljeni. Zbog takve prirode digitalnih podataka od velike je važnosti poštovati proceduru pribavljanja digitalnih dokaza te njihova obrada i pravilna prezentacija tokom krivičnog ili nekog drugog postupka. Takođe, postupak prilikom izuzimanja zatečenih mobilnih telefona, kao mogući izvor dokaza, sa mesta izvršenja krivičnog dela mora biti zasnovan na pravilnom postupanju i zakonski propisanim procedurama [6].

Čitav proces forenzike mobilnih telefona sastoji se od sledećih faza: očuvanje, prikupljanje, ispitivanje, analiza i izveštavanje.

- Faza očuvanja je prva faza u procesu digitalnog povraćaja podataka i podrazumeva oduzimanje i obezbeđivanje imovine osumnjičenog bez menjanja sadržaja podataka na uređajima. Nakon oduzimanja uređaja sa ciljem sprečavanja izmene sadržaja, ukoliko je telefon uključen, važno je izvršiti mrežnu izolaciju. Poželjno je telefon odložiti u Faradej kutiju/vrećicu ali i onemogućiti sve mrežne veze (Wi-Fi, GPS, Hotspot, itd) i aktivirati režim letenja.
- Prikupljanje (akvizicija) je druga faza u kojoj se sakupljaju informacije sa digitalnih uređaja. Podrazumeva identifikaciju i ekstrakciju podataka. Cilj ove faze je preuzimanje podataka sa mobilnog uređaja. Zaključani ekran može se otključati sa odgovarajućim PIN-om, lozinkom, uzorkom ili biometrijom. Problem predstavlja mobilnost podataka jer oni zapravo mogu biti na drugoj lokaciji. Tu spada i Cloud okruženje, vrlo popularno kod mobilnih korisnika.
- Ispitivanje i analiza imaju za cilj da potvrde ili demantuju pretpostavke vezane za slučaj. Da iz mnoštva dokaza povežu relevantne za konkretan slučaj i formiraju sliku događaja.
- Izveštavanje se oslanja na detaljan pregled svih preduzetih koraka i donetih zaključaka tokom istrage. Prezentuju se rezultati testiranja i ispitivanja i daju objašnjenja do kakvih se zaključaka došlo na osnovu prikupljenih dokaza.

Od svih navedenih faza prve dve se smatraju najvažnijim. Očuvanje i prikupljanje mogu da obezbede ključne dokaze i značajne smernice za nastavak istrage. Svaki korak mora biti sproveden sa izuzetnom pažnjom jer naredne faze ispitivanja u potpunosti zavise od toga koliko dobro su obavljene prve dve faze [7].

A. Metode ekstrakcije

Ekstrakcija podataka je postupak prikupljanja podataka, sa medija sa podacima, za dalju obradu. U digitalnoj forenzici mobilnih uređaja ovaj postupak je obavezan i većini slučajeva izuzetno značajan jer omogućava dokaze ili druge važne podatake koji upućuju na dalje dokaze [8]. O vrsti ekstrakcije koja će se primeniti u konkretnom slučaju odlučuje sam forenzičar. Odluku donosi pre svega na osnovu, tipa uređaja sa kojim radi, njegovog zatečenog stanja (ispravan, oštećen, zaključan i sl), količine i vrste podataka koje želi izvući i forenzičkog alata / mogućnosti kojima raspolaže. Vrlo često, u praksi, važan faktor koji utiče na odluku, je i vreme jer je ponekad važnije hitnije doći do određenih podataka pre nego do svih. Najjednostavnijim metodama se može dobiti najmanje podataka, ali su najbrže, dok se najkomplikovanijim metodama može dobiti najviše podataka, ali je postupak dugotrajan, treba ispuniti posebne uslove u kojima se obavlja i skupu opremu te stručno osoblje i zbog toga je rezervisana za službe kao što su policija i vojska ili agencije koje se bave digitalnom forenzičkom analizom.

- Ručna ekstrakcija, najjednostavnija metoda koja podrazumeva snimanje (obično digitalnom kamerom) sve informacije koje je moguće videti na ekranu mobilnog uređaja. Jasno je da metoda efikasna samo u malom broju specifičnih sučajeva jer ne nudi podatke izbrisane sa uređaja kao i ni podatke kojima se ne može pristupiti kroz sistem menija.
- Logička ekstrakcija je nakon ručne najlakša i najkompatiblnija metoda ali povlači manji broj podataka od fizičke. Ovaj pristup podrazumeva uspostavljanje veze između mobilnog uređaja i forenzičke radne stanice najčešće pomoću USB kabla, ali i preko Bluetooth-a, infrared ili RJ-45 kabla. Većina forenzičkih alata podržava logičku ekstrakciju, a sam proces je relativno jednostavan i zahteva kratkotrajnu obuku. Nedostatak ove tehnike je što u zavisnosti od telefona i forenzičkih alata koji se koriste, kao rezutat ne daje sve već samo neke od podataka i ne omogućava pristup izbrisanim podacima.
- Fizičkom ekstrakcijom se dobija se najviše podataka što uključuje podatke o lokaciji i specifične dokumentacije za aplikacije. Da bi se izvršila fizička ekstrakcija neophodno je otključati uređaj i biti u mogućnosti (tehnički i zakonski) da instalirate jailbreak. Za sada je „Jailbreaking“ moguć za većinu verzija iOS-a do 11.1.2, ali ne i za iOS 11.2 ili noviju verziju [9]. Za razliku od konvencionalnih logičkih procesa ekstrakcije, fizička metoda zaobilazi operativni sistem telefona, prikupljajući podatke direktno iz

unutrašnje flash memorije telefona. Neraspodeljeni prostor može sadržati pristup izbrisanim stavkama kao što su SMS, dnevnici poziva, imenik, slike i video zapisi.

- Ekstrakcija Clouda je novija metoda koju obavezno treba uvrstiti jer iako spada u izazove u velikoj meri pomaže u količini sakupljenih podataka te formiranju detaljnije slike. Problem predstavlja činjenica da je Cloud distribuirano okruženje te da računari od inetersa nisu na istoj geografskoj lokaciji. Pored toga često je potrebno doći i do mrežnih zapisa kako bi se utvrdilo kada je podatak postavljen na Cloud. Olakšavajuća okolnost je to što se ne zahteva pristup samom uređaju i nije bitno da li je uređaj zaključan ili ne.

III. IZAZOVI

Jedan od najvećih forenzičkih izazova kada je u pitanju mobilna platforma je činjenica da se podacima može pristupiti i da se mogu čuvati i sinhronizovati sa/na više uređaja. Kako su podaci ranjivi te se mogu brzo transformisati ili brisati daljinski, potrebno je mnogo više napora za njihovo očuvanje. Neki do izazova su:

- Hardverske razlike - Tržište je preplavljeno različitim modelima mobilnih uređaja različitih proizvođača. Novi modeli se pojavljuju izuzetno često što zaista predstavlja izazov za forenzičare koji moraju biti u toku sa svim promenama. Osim toga, ugrađen prostor za skladištenje nije jednostavno ukloniti sa uređaja, za razliku od tradicionalnih desktop računara i servera [10].
- Mobilni operativni sistemi - Za razliku od personalnih računara u kojima Windows već godinama dominira na tržištu, mobilni uređaji koriste različite operativne sisteme, uključujući Appleov iOS, Google Android, RIM BlackBerri OS, Microsoftov Windovs Mobile, HP's vebOS, Nokia Simbian OS i druge. Pored ovolikog broja OS čak i u okviru njih postoje različite verzije.
- Ugrađena sigurnost - Ugrađene bezbednosne funkcije pametnog telefona prisutne su na mnogim nivoima kako bi se zaštitili podaci i privatnost korisnika. Načini zaključavanja u današnjim pametnim telefonima mogu se razlikovati od jednostavnog četvorocifrenog PINa do mnogo kompleksnijih i dugačkih kodova, šablona zaključavanja ili biometrije. Novije OS verzije nude potpunu enkrpiciju diska, što može biti izuzetno problematično prilikom pokušaja akvizicije podataka.
- Cloud - Zbog generisanja velike količine podataka, uštede prostora za skladištenje ili potrebe za rezervnim kopijama, korisnici biraju da čuvaju puno važnih podataka u oblaku. Problem može nastati ne samo zbog tehničke prirode već i zakonske regulative. U izveštaju NIST Cloud Computing Forensics Science Working group, govori se o 65 izazova od kojih spadaju, u devet glavnih kategorija, pored navedene arhitekure i zakonske regulative takođe i antiforenzika, načini sakupljanja i analize podataka, obuka, standardi [11].
- Ranjivost podataka - Generalna osobina digitalnih podataka je da mogu biti ranjivi ali to posebno dolazi do izražaja kod mobilnih uređaja. Digitalni dokazi se mogu lako menjati (sa namerom ili bez) skroz modifikovati i umnožavati bez ostavljanja traga. Prilikom mrežnog prenosa informacija može biti modifikovana ili izgubljena [7]. Stoga je od izuzetne važnosti izolovati telefon kako bi se sprečio gubitak podataka ili njihova modifikacija.
- Nepostojanje mehanizma za blokiranje "pisanja"'čini ekstrakovane podatke manje uverljivim .

IV. ANDROID & IOS

Razmatranje OS sa forenzičkog aspekta podrazumeva poznavanje sigurnosnog modela. Svi odgovorni proizvođači brinu o sigurnosti podataka svojih korisnika te je, u većini slučajeva, implementirani sigurnosni model prepreka za forenzičara.

Android je operativni sistem zasnovan na Linux-u sa otvorenim kodom, koji je razvila kompanije Android Inc. 2003. godine. Google ga je otkupio 2005. predstavio 2007. S obzirom da je otvoren i besplatan pogodan je za kompanije koje zahtevaju jeftini, prilagodljiv i lagan operativni sistem za svoje pametne uređaje, bez razvoja novog operativnog sistema od nule. Android ima mogućnost istovremenog pokretanja više aplikacija a svaka aplikacija je digitalno potpisana i izolovana u svom sopstvenom "sandbox-u". Svaki "sandbox" definiše privilegije svoje aplikacije. Iznad kernela, sve aktivnosti imaju ograničeni pristup sistemu. Android koristi algoritme industrijskog standarda za pružanje kriptografije i sposobnosti zaštite podataka kako bi se osigurale tri glavne funkcije: šifrovanje uređaja, sigurnost aplikacija i mrežno povezivanje i šifrovanje (SSL, VPN i Wi-Fi) [12]. Dva glavna problema koja se mogu izdvojiti u vezi ugrožavanja bezbednosti kod Android OS su takozvana eskalacija privilegija (aplikacije sa ograničenim skupom dozvola komuniciraju medju sobom sa indirektnim privilegijama što potencijalno omogućava izvršavanje neovlašćenih postupaka) i curenje privatniih podataka [13].

iOS, ranije poznat i kao iPhone operativni sistem, je mobilni operativni sistem razvijen i distribuiran isključivo od strane Apple Inc. Univerzalan je za sve Apple mobilne uređaje, kao što su iPad, iPod touch i iPhone. Kao što je već navedeno iOS uređaji čuvaju podatke na NAND flash memorijskim čipovima unutar uređaja. Ono što ih razlikuje od mnogih drugih mobilnih uređaja je što nemaju prenosivu bateriju ili slotove za eksterno skladištenje. Svi podaci korisnika se čuvaju u NAND i koristi se HFS+ sistemski fajl. Ovaj zatvoreni dizajn je u skladu sa ostalim Apple proizvodima [14]. Apple ima namenski kriptografski čip koji omogućava enkripciju zasnovanu na hardveru, i integrisan je na svim iOS uređajima. Ova funkcija uključivanja kriptografije u OS, pre svega, ima za

cilj zaštitu podataka te omogućava šifriranje ili dešifrovanje bilo koje datoteke ili deo datoteke koristeći poseban ključ [8].

Android i iOS uređaji podjednako čuvaju svoje podatke na internim NAND flash memorijskim čipovima. Jedna od najvažnijih razlika između Android i iOS uređaja je da Android smartfoni, za razliku od iPhone-a, imaju i eMMC čipove i izmenjive SD kartice za dodatno skladištenje. Podaci iz aplikacija na uređaju se mogu podeliti na interni eMMC čip i na prenosivu memorijsku karticu, što komplikuje zadatke forenzičke analize. Android O/S može da koristi ili Linux 2.6 kernel ili SELinux kernel, koji obezbeđuje dodatnu bezbednosnu kontrolu. Postoje tri vrste najčešće korišćenih Linux sistemskih fajlova, iako Android uređaj može koristiti bilo koji od brojnih Linux fajlova koji su dostupni. Ext4, najčešći na većini novih Android uređaja. YAFFS2, sistemski fajl otvorenog koda namenjen za uređaje koji koriste fleš memoriju, koristi napredne mere "sakupljanja smeća" kako bi brže počistio izbrisane podatke, što može da ugrozi rad forenzičara [15].

Uočljivi trend kod iOS uređaja je kontinuirani rad na povećanju sigurnosti kod svakog narednog modela. Forenziku je lakše izvoditi na starijim uređajima sa čipom A_4 i manjim (uključuje sve uređaje isporučene pre iPhone 4s). iOS uređaji besplatno pružaju mogućnost pravljenja rezervnih kopija podataka, kao što su iTunes i iCloud kao i funkciju "FindMyiPhone". Prilikom izuzimanja ovakvih uređaja izuzetno je važno da se izoluju od bilo kog daljinskog pristupa, jer se ova usluga može koristiti i za daljinsko brisanje podataka. Sa druge strane postojanje kopije podataka na Cloudu može biti od velike pomoći za forenzičku istragu. Kod Android korisnika takođe postoji mogućnost povezivanja uređaja sa svojim Google nalogom ali većina Android uređaja ne radi kopiju podataka automatski. Ako korisnik izabere ovu opciju, podaci sa telefona mogu biti snimljeni i sačuvani na Google Cloud-u.

Prednost iOS uređaja, koju treba izdvojiti, je da ako želimo instalirati špijunski softver na iOS uređaju se mora uraditi „Jailbreaking“. "Jailbreaking" uređaja znači korištenje softvera unutar operativnog sistema uređaja kako bi uklonio određena ograničenja na uređaju [16].

V. EKSTRAKCIJA PODATAKA PRIMENOM CELEBRITE - UFED

Svakodnevni dramatični porast broja podataka kao i njihova raznovrsnost u velikoj meri utiču na uspešnost ekstrakcije. Informacije koje je moguće sakupiti sa mobilnih uređaja razlikuju se u zavisnosti od izabranog modela ekstracije, alata koji se koristi i konkretnog uređaja na kome se primenjuje. Zbog navedenih specifičnosti presek trenutnih mogućnosti mobilne forenzike je najbolje sagledati iz izveštaja samih proizvođača. Jedan od lidera u ovoj oblasti je izraelska kompanija Cellebrite te su mogućnosti njihovog rešenja Cellebrite - UFED dobar pokazatelj stanja u ovoj oblasti.

U tabeli I dat je pregled rezultata ekstrakcije UFED-a 6.5 (najnovije verzije u trenutku pisanja rada) [17]. Tabela predstavljena u radu je samo deo izvorne tabele, detaljan pregled svih ekstrakovanih podataka moguće je pronaći na sajtu proizvođača.

TABELA I. CELLEBRITE UFED ULTIMATE V6.5 SUPPORTED PHONES LIST

Vendor	**Apple**		**Samsung GSM**
Model	***iPhone 4 (A1349)***	***iPhone X (A1902)***	***SM-N950F Galaxy Note 8***
Physical Extraction	Y		Y
Physical Bypassing Lock	Y		
Physical Dump Methods			ADB (Rooted); Advanced ADB (Generic)
File System Extraction	Y	Y	Y
Bluetooth Address	Y	Y	
Bluetooth Devices	Y	Y	Y
Calendar	Y	Y	Y
Calls	Y	Y	Y
Contacts	Y	Y	Y
Cookies	Y	Y	Y
Emails	Y-P Y-FS-Only_ Jailbroken	Y-FS-Only_ Jailbroken	Y
Installed Applications	Y	Y	Y
IP Connections	Y	Y	
Locations	Y	Y	Y
MMS	Y	Y	Y
Notes	Y	Y	Y
Passcode			Y
Phone Number	Y	Y	
SMS	Y	Y	Y
User Accounts	Y	Y	Y
User Dictionary	Y	Y	Y
Voicemail	Y	Y	
Web History	Y	Y	Y
Wi-Fi Address	Y	Y	
Wi-Fi Networks	Y	Y	Y
Booking.com	Y	Y	Y
Chrome	Y	Y	Y
Dropbox	Y	Y	Y
Facebook	Y	Y	Y
Facebook Messenger	Y	Y	Y
Firefox	Y	Y	Y
Gmail	Y	Y	Y
Google Docs	Y	Y	Y

Vendor	Apple		Samsung GSM
Model	*iPhone 4 (A1349)*	*iPhone X (A1902)*	*SM-N950F Galaxy Note 8*
Google Drive	Y	Y	Y
Google Duo	Y	Y	Y
Google Maps	Y	Y	Y
Inbox	Y	Y	Y
Instagram	Y	Y	Y
InstaMessage	Y	Y	Y
LinkedIn	Y	Y	Y
Pinterest	Y	Y	Y
Skype	Y	Y	Y
Snapchat	Y	Y	Y
Tinder	Y	Y	Y
TripAdvisor	Y	Y	Y
Twitter	Y	Y	Y
Uber	Y	Y	Y
Viber	Y	Y	Y
WeChat	Y	Y	Y
WhatsApp	Y	Y	Y
Yahoo Mail	Y	Y	Y
Yahoo Search	Y	Y	Y
Yahoo! Messenger	Y	Y	Y
YouTube	Y	Y	Y

U ovom pregledu testirana su dva modela na iOS platformi - iPhone 4 (A1349) i iPhone X (A1902) kao i jedan na Android - SM-N950F Galaxy Note 8. Razlog za postojanje starijeg modela iPhone uređaja je da bi se pokazali podaci dobijeni fizičkom ekstrakcijom koja nije moguća na modelu iPhone X, što se vidi već u prvoj koloni sa podacima ekstrakovanja.

Sama tabela je vrlo pregledna te je nije neophodno dodatno komentarisati, lako je uočiti je da je većina aplikacija podržana kod sva tri modela. Ono što treba izdvojiti je da iako je moguće kod svih testiranih modela iščitati Bluetooth uređaje i Wi-Fi mreže, samo kod Apple uređaja postoji informacija o Bluetooth i Wi-Fi adresi. To isto važi i za IP Connections, ostavljaju trag samo na iPhone. Takođe, očigledno je da je fizička ekstracija moguća kod najnovijeg Android modela što nije slučaj sa iOS, što potvrđuje tvrdnju komapnije Apple da je njima sigurnost prioritet. U prilog tvrdnji je i činjenica da je Passcode iščitan samo na Android uređaju.

VI. ZAKLJUČAK

Mobilni uređaji su odavno prevazišli kategoriju uređaja koji nude osnovne informacije o korisniku. Zadivljujućim podacima o istoriji poziva, listi kontakata, SMS poruka, sa pojavom pametnih uređaja, pridružili su se podaci o lokaciji i kretanju korisnika, instaliranim i obrisanim aplikacijama, bežičnim mrežama, društvenim mrežama, listi pretraga, lozinki i sl. Mobilni uređaj je postao izuzetna podrška u istrazi i prikupljanju dokaza čak i za sofisticirano profilisanje korisnika te predikciju potencijalnih namera i planiranih aktivnosti.

Uprkos činjenici da postoji mnoštvo podataka i dosta različitih metoda ekstrakcije brojni izazovi koji se stavljaju pred mobilnog forenzičara mogu uticati na količinu prikljupenih podataka i brzinu rada. Hardverske i softverske razlike kod različitih proizvođača su očekivane ali se pojavljuju i kod istih modela uređaja na unapređenim verzijama. Ranjivost podataka je potencijalno ugrožena bežičnim pristupom a Cloud rešenja, iako mogu biti dobra alternativa, forneziku mobilnih uređaja čine još zahtevnijom. Sami proizvođači mobilnih uređaja konstantno unapređuju zaštitu podataka na svojim uređajima te dodatno otežavaju ekstrakciju podataka. U tim nastojanjima, definitivno prednjači kompanija Apple čiji su noviji uređaji, što se vidi i na osnovu podataka iz tabele ekstrakovanih podataka, zaštićeni od fizičke ekstrakcije. Primenjena enkripcija je toliko snažna da se čak i sama kompanija izjasnila da ne može da je probije.

Može se reći da je zlatno doba mobilne forenzike prošlo. Nema više jednostavnog i lakog načina za dobijanje podataka iz novijih telefona. S obzirom na zaštitu koju primenjuje kompanija Apple verovatno je da će se mobilna forenzika fokusirati na ekstrakciju podataka sa Cloud-a (iCloud). Kod Androida je trenutno još uvek moguća fizička ekstrakcija ali uz trend povećanja nivoa zaštite realno je očekivati da će uskoro i za Andorid ekstrakcija sa Cloud-a biti alternativno rešenje.

Dalja istraživanja, u skladu sa zaključenim, trebalo bi fokusirati na forenzici Cloud-a uz konstantno praćenje novih metoda zaštite, pre svega iOS, te potencijalnih ranjivosti.

LITERATURA

[1] Meyers, J. Watch the incredible 70-year evolution of the cell phone, http://www.businessinsider.com/complete-visual-history-of-cell-phones-2011-5; [accessed 10.01.18].

[2] Number of smartphone users worldwide from 2014 to 2020, https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/; [accessed 10.01.18].

[3] Gartner Says Worldwide Sales of Smartphones Grew 9 Percent in First Quarter of 2017; https://www.gartner.com/newsroom/id/3725117 [accessed 10.01.18].

[4] Gartner Says Worldwide Device Shipments Will Increase 2.1 Percent in 2018, https://www.gartner.com/newsroom/id/3849063; [accessed 10.01.18].

[5] Jansen W, Ayers R. Guidelines on cell phone forensics. NIST Special Publication. 2007;800:101.

[6] Kaurin, T. Skakavac Z. "Značaj digitalne forenzike mobilnih uređaja u otkrivanju i dokazivanju krivičnih dela organizovanog kriminaliteta", Zbornik radova 5. Međunarodne znanstveno-stručne konferencije - Istraživački dani Visoke policijske škole u Zagrebu Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda, Zagreb, Hrvatska, pp. 58-82, 21. - 22. travnja 2016.

[7] Kaurin, T., Anucojić, D. "Smernice za izbor alata digitalne forenzike", Infoteh, Jahorina, , pp. 715-720, Mart 21-23, 2012.

[8] T. Kechadi, M. Faheem, N. An Le-Khac, "The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and

Current Trends," International Journal of Digital Crime and Forensics, vol. 7, Issue 2, pp. 1-19, April 2015

[9] S. Tahiri, Mastering Mobile Forensics. Packt Publishing, 2016

[10] D. Lillis, B. Becker, T. O'Sullivan, M. Scanlon, *Current Challenges and Future Research Areas for Digital Forensic Investigation*, 2016. https://arxiv.org/abs/1604.03850 [accessed 02.03.18]

[11] NIST. NIST Cloud Computing Forensic Science Challenges. 2014. https://csrc.nist.gov/publications/detail/nistir/8006/draft; [accessed 10.01.18].

[12] Android forensic, https://www.gillware.com/forensics/mobile/ android - forensics-services/ ; [accessed 10.01.18].

[13] Bhandari S, Jaballah W, Jain V, Laxmi V, Zemmari A, Gaur M, Mosbah M, "Android inter-app communication threats and detection techniques" Computers and Security, vol. 70 (2017) pp. 392-421 Published by Elsevier Ltd

[14] iOS forensics, https://www.gillware.com/forensics/mobile/ios-forensics/; [accessed 10.01.18].

[15] E. R. Mumba and H. S. Venter, "Mobile forensics using the harmonised digital forensic investigation process," 2014 Information Security for South Africa, Johannesburg, 2014, pp. 1-10.doi: 10.1109/ISSA.2014. 6950491.

[16] Meet iOS 11.3: Apple to Make It Harder for Law Enforcement to Extract iPhone Data, https://blog.elcomsoft.com/2018/01/meet-ios-11-3-apple-to-make-it-harder-for-law-enforcement-to-extract-iphone-data/; [accessed 15.01.18].

[17] Highlights-Cellebrite, https://media.cellebrite.com/wp-content/uploads/ 2018/01/ UFED6.5_ReleaseNotes.pdf; [accessed 20.01.18].

ABSTRACT

Digital devices have become part and parcel of our lives. Their intensive usage in every aspect as well as their extremely detailed activity tracking abilities turn them into their owners' behavioral digital data bases. In digital devices' widest diversity, it is mobile phones definitively proving to be their owners' daily companions, their lives' vital data guardians – both the realities thereof and their hidden desires, preferences and plans. Enormous data processing capabilities enable user profile creation, prove location(s) and perpetrated activities as well as surmise those that will potentially happen, putting them in top layer of digital forensics eligible devices. Even though current mobile forensics market tools offer impressive amount of collectible data, one has to be aware of real possibilities, possible obstacles as well as challenges.

Present paper's aim is to highlight multitude of existing and rapidly growing challenges in the field mainly as a result of a high level manufacturer data protection, as well as point to trends and tendencies of mobile forensics development by analyzing current state and presenting data extraction capabilities of the two market's most popular mobile platforms (iOS and Android).

MOBILE DEVICES' FORENSICS OPPORTUNITIES AND CHALLENGES

Tanja Kaurin