Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.738.5:341.1
DOI: https://doi.org/10.24867/11BE14Maravic

DIGITALNA FORENZIKA iOS UREĐAJA

DIGITAL FORENSICS OF iOS DEVICES

Jelena Maravić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIČKO I RAČUNARSKO INŽENJERSTVO

Kratak sadržaj – *U ovom radu obrađena je digitalna forenzika sa akcentom na digitalnu forenziku iOS uređaja. Kako digitalna forenzika podrazumeva primenu naučnih metoda na obezbeđivanje digitalnih dokaza, u radu su obrađene sve faze koje obuhvataju jednu digitalnu forenzičku istragu i detaljno su opisane tehnike ekstrakcije podataka iz iOS uređaja i alati koji implementiraju te tehnike.*

Ključne reči: *digitalna forenzika, iOS, tehnike, procesi, alati*

Abstract – *This paper addresses the theme of digital forensics with an emphasis on digital forensics of iOS devices. As digital forensics implies the application of the scientific method to provide digital evidence, the paper deals with all phases that include a single digital forensic investigation and describes in detail the techniques of data extraction from iOS devices and tools that implement these techniques.*

Keywords: *digital forensics, iOS, techniques, processes, tools*

1. UVOD

U istoriji mobilnih uređaja ostaće zapamćeno da na samom početku nisu bili prihvaćeni od strane korisnika i da je broj kupaca bio veoma mali. Kako se, iz godine u godinu, radilo na njihovom unapređenju i razvoju tako je rastao i broj korisnika.

Telefoni su postali nezaostavni deo ljudske svakodnevnice. Uređaj kao takav ima sposobnost memorisanja aktivnosti sa ekstremnim detaljima što ga pretvara u digitalnu bazu podataka ponašanja njegovih korisnika.

Sveprisutnost mobilnih uređaja ubrzala je razvoj i usavršavanje i zlonamernih radnji na čiji put se trudi stati digitalna forenzika. Digitalna forenzika se bavi pribavljanjem što većeg broja podataka koje je teško ili nemoguće obezbediti na neki drugi način.

Prvi deo ovog rada bavi se digitalnom forenzikom, njenom istorijom i procesima. Forenzika mobilnih uređaja, kao jedna od bitnih grana digitalne forenzike, obrađena je u narednom odeljku.

Nakon toga, opisan je iOS operativni sistem sa pogledom na njegovu arhitekturu, fajl sistem, sigurnost i tehnike i metode akvizicije podataka. Zatim, sledi primer korišćenja određenog forenzičkog alata pomoću koga se vrši pronalazak lozinke kako bi se dekriptovali enkriptovani podaci rezervne kopije uređaja. Na samom kraju, dat je pogled na temu budućeg razvoja digitalne forenzike mobilnih uređaja.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Stevan Gostojić, vanr. prof.

2. DIGITALNA FORENZIKA

Postoji više definicija digitalne forenzike ali ona koja je najčešće pominjana je definicija Radne grupe za istraživanje digitalne forenzike iz 2001. godine i ona glasi: „Digitalna forenzika podrazumeva upotrebu naučno-izvedenih i potvrđenih metoda radi očuvanja, prikupljanja, validacije, identifikovanja, analize, tumačenja, dokumentovanja i predstavljanja digitalnih dokaza izvedenih iz digitalnih izvora za potrebe omogućavanja ili poboljšanja rekonstrukcije krivičnog događaja [1].“

2.1. Istorija digitalne forenzike

Razvoj personalnih računara 1970-tih godina prošlog veka je doveo do povećanja broja korisnika kako su postali dostupniji sve širem krugu ljudi. Sa razvojem računara, razvijao se i povećavao broj njegovih zloupotreba u kriminalne svrhe.

Prvi zabeleženi slučajevi zloupotreba vezani su za finansijske prevare i povrede prava intelektualne svojine. Kao potreba da se prikupe dokazi za gonjenje i suđenje, u ovakvim slučajevima zloupotrebe informacionih tehnologija, nastala je digitalna forenzika.

Kroz godine, nastajale su razne organizacije i asocijacije čiji je glavni zadatak bio razvoj, pronalaženje najboljih praksa i definisanje standarda računarske forenzike. Rezultat ovoga bilo je stvaranje Međunarodne organizacije za računarske dokaze (Internacional Organization on Computer Evidence) čiji je zadatak bio da izradi međunarodne principe i vodiče za postupanje sa digitalnim dokazima [1].

„Zlatno doba digitalne forenzike“ vezano je za period od 1999. do 2007. godine kada se ova disciplina posmatrala kao svemoguća za oporavak podataka i rekonstrukciju događaja u prošlosti u digitalnom okruženju [1].

Od tada do danas se dosta toga promenilo. Forenzičari se susreću sa sve boljim i sofisticiranijim uređajima za koje moraju praviti još bolje alate kako bi nesmetano izvršili istragu i sačuvali integritet dokaza.

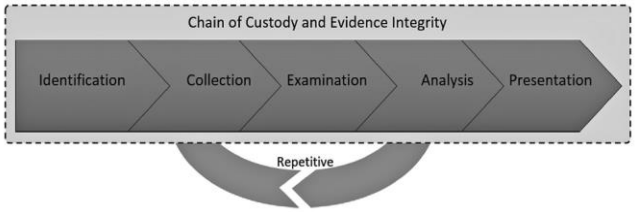
2.2. Procesi u digitalnoj forenzici

Digitalni dokazi se mogu pronaći u računarima, mobilnim uređajima, internet infrastrukturama, industrijskim sistemima i u drugim digitalnim uređajima. Primena forenzičkih procesa i njenih principa će osigurati da istraga bude forenzički ispravna. Dva osnovna principa, koja se moraju ispoštovati, jesu:

- **Integritet dokaza** - odnosi se na čuvanje dokaza u njihovoj originalnoj formi – ne sme biti izmena,
- **Lanac nadzora** (chain of custody) – odnosi se na to da mora postojati mogućnost dokumentovanja svih odrađenih akcija nad dokazom kako bi se dokazala njegova autentičnost i integritet.

Istražni proces u digitalnoj forenzici se sastoji od pet faza (slika 1) koje su zasnovane na principima digitalne forenzike, zakonima sprovođenja i najboljim praksama a to su:

1. **Identifikacija** – dokazi mogu biti identifikovani na osnovu žalbi, upozorenja ili na osnovu nekih drugih naznaka. Ova faza se može iskoristiti kako bi se identifikovali dokazi ili objekti kojima se treba posvetiti tokom istrage. Identifikacija vodi do formiranja hipoteze o digitalnim uređajima ili sistemima koji možda sadrže potencijalne digitalne dokaze.
2. **Prikupljanje** – odnosi se na nabavku i kopiranje podataka. Ovo je vezano za situaciju kada istražitelj dobije pristup digitalnom uređaju koji sadrži sirove podatke koji su identifikovani kao relevantni za konkretni slučaj.
3. **Pregled** – svi prikupljeni podaci moraju biti pregledani i pripremljeni za kasniju analizu. U ovoj fazi se često može zahtevati i obnavljanje, parsiranje i pretprocesiranje sirovih podataka kako bi postali razumljivi za forenzičke istražitelje u narednoj fazi.
4. **Analiza** – služi da forenzički istražitelji utvrde koji digitalni objekti će se koristiti kao digitalni dokazi kako bi potvrdili ili opovrgnuli hipotezu kriminalnog slučaja, incidenta ili događaja.
5. **Prezentacija** – uključuje finalnu dokumentaciju i prezentaciju rezultata istrage koja će se predstaviti sudu ili nekoj drugoj instituciji/organizaciji. Prezentacija dokaza podrazumeva objektivne dokaze koji su dovoljno jasni.



Slika 1 – *Faze digitalnog forenzičkog procesa* [2]

3. FORENZIKA MOBILNIH UREĐAJA

3.1. Proces forenzike mobilnih uređaja

Proces forenzike mobilnih telefona se sastoji od sledećih faza: očuvanja, prikupljanja, ispitivanja, analize i izveštavanja.

U fazi očuvanja, prvi koraci vezani su za obezbeđenje mobilnog telefona, kako ne bi došlo do menjanja sadržaja na uređaju. Ukoliko je telefon uključen, važno je izvršiti mrežnu izolaciju. Nakon izolacije telefona, može se preći na fazu prikupljanja podataka. Forenzička akvizicija i izvlačenje podataka sa mobilnih telefona je jedan od najzahtevnijih postupaka istrage zbog brze promene u hardverskoj i softverskoj strukturi i velikog broja prisutnih nestandardnih uređaja na tržišu. 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 faza u procesu digitalne forenzike mobilnih telefona, dve se smatraju kao najznačajnije – obezbeđuju dokaze i značajne smernice za nastavak istrage, a to su očuvanje i prikupljanje podataka.

3.2. Tehnike za forenziku mobilnih uređaja

Tehnike koje se mogu koristiti u fazi prikupljanja podataka na mobilnim uređajima su:

1. Ručna ekstrakcija podataka
2. Logička ekstrakcija podataka
3. Fizička ekstrakcija podataka
4. Cloud ekstrakcija podataka

Ručna ekstrakcija je najjednostavnija metoda koja podrazumeva snimanje, koje je obično digitalnom kamerom, svih informacije koje je moguće videti na ekranu mobilnog telefona. Metoda je manje efikasna jer ne nudi podatke koji su izbrisani sa uređaja kao ni podatke kojima se ne može pristupiti kroz sistem menija. Nedostatak je i što se ovom tehnikom ne može očuvati integritet uređaja.

Logička ekstrakcija podrazumeva uspostavljanje veze između mobilnog telefona i forenzičke radne stanice, najčešće pomoću USB kabla, ali i preko Bluetooth-a. Da bi se logička ekstrakcija mogla izvršiti, potrebno je otključati telefon. Određeni alati omogućavaju da se, bez otključavanja telefona, dobije određena mala količina podataka. Mana ove tehnike je to što povlači manji broj podataka od fizičke ekstrakcije i što nema mogućnost povraćaja izbrisanih podataka. Većina forenzičkih alata podržava logičku ekstrakciju, a sam proces je veoma jednostavan i zahteva kratkotrajnu obuku.

Po količini preuzetih podataka, između logičke i fizičke ekstrakcije nalazi se **datotečna ekstrakcija**. Ona pronalazi sve datoteke koje su pohranjene u delu memorije uređaja koji se smatra zauzetim. Pomoću nje, mogu se videti i neki podaci koje je korisnik izbrisao.

Fizičkom ekstrakcijom se dobija najviše podataka jer se vrši kopiranje svakog bita koji se nalazi na fizičkom uređaju. Ova tehnika, za razliku od logičke ekstrakcije, zaobilazi operativni sistem telefona, prikupljajući podatke direktno iz unutrašnje fleš memorije telefona. Neraspodeljeni prostor može sadržati pristup izbrisanim stavkama kao što su SMS, dnevnici poziva, imenik, slike i video zapisi.

Ekstrakcija cloud-a je najnovija metoda koja je veoma izazovna ali u velikoj meri pomaže u količinih sakupljenih podataka i formiranju detaljnije slike. Problem kod ove tehnike je činjenica da je cloud distribuirano okruženje te da računari od interesa nisu na istoj geografskoj lokaciji. Olakšavajuća okolnost je što ne zahteva pristup samom uređaju i nije bitno da li je uređaj zaključan ili ne.

3.3. Metode za forenziku mobilnih uređaja

Pored nabrojanih tehnika, postoje razne metode koje tehnike koriste kako bi ekstrakcija bila izvršena a to su:

- Ručna ekstrakcija
- Metode logičke ekstrakcije:
  - SIM ekstrakcija - Kako bi se podaci iz SIM kartice preuzeli, potrebno je posedovati softver i čitač kartica. Velika je verovatnoća da će se dobijeni podaci morati srediti za pregled.
  - Rezervna kopija - određeni uređaji, posebno telefoni, mogu imati rezervne kopije na računaru ili

nekom drugom mestu (cloud). Ovi podaci mogu biti enkriptovani. Za pregled ovih podataka, pored raznih forenzičkih alata, moguće je koristiti iTunes.

- Metode fizičke ekstrakcije:
  - Hex dumping/JTAG - kada ne postoji niti jedan drugačiji način za forenzičko ispitivanje mobilnog uređaja, prelazi se na JTAG interfejs. JTAG kontakti na uređajima su prvenstveno namenjeni testiranju rada hardvera na uređajima, mada se mogu koristiti i da bi se pristupilo fleš memoriji uređaja. Iščitavanjem kompletnog sadržaja memorije preko JTAG interfejsa dobija se kompletan forenzički dokazni materijal, koji u daljoj obradi može biti analiziran ili sačuvan za neku dalju obradu.
  - Chip-off je metoda forenzičke ekstrakcije podataka koja uključuje fizičko uklanjanje flash memorije uređaja na kojem se vrši analiza.
  - Micro read je metoda ekstrakcije podataka koja uključuje pregled memorije uređaja pod elektronskim mikroskopom. Ova metoda je veoma spora, zahteva sofisticiranu tehničku opremu (elektronski mikroskop) i potreban je tim stručnjaka kako bi se sprovela.

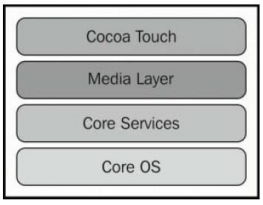
4. iPhone operating system – iOS

iOS je mobilni operativni sistem razvijen i distribuiran od strane Apple Inc. Univerzalan je operativni sistem za sve Apple uređaje kao što su Apple TV, iPad, iPod Touch i iPhone. Izveden je iz OS X, koji je baziran na sistemu Darwin BSD-u i stoga pripada grupi juniksolikih operativnih sistema. Upravlja hardverom uređaja i pruža tehnologije potrebne za implementaciju nativnih aplikacija.

4.1. iOS arhitektura

iOS se ponaša kao posrednik između osnovnih hardverskih komponenti i aplikacija koje se pojavljuju na ekranu. Aplikacije ne komuniciraju direktno sa osnovnim hardverskim komponentama, već se njihova komunikacija odvija preko dobro dizajniranog sistemskog interfejsa koji štiti aplikacije od hardverskih promena.

iOS arhitektura (slika 2) se sastoji od četiri sloja: kakao dodir sloj (cocoa touch layer), medija sloj, sloj osnovnih usluga i osnovni sloj.



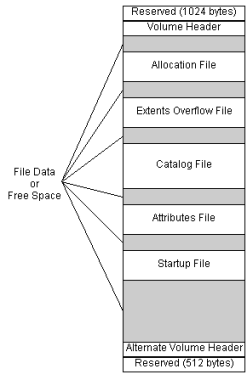
Slika 2 - *iOS slojevi* [2]

4.2. iOS fajl sistem

Fajl sistem koji se koristi na iPhone-u i drugim iOS uređajima je HFSX (Hierarchical File System) koji predstavlja varijaciju HFS Plus-a. HFSX razlikuje mala i velika slova dok ih HFS Plus ne razlikuje. OS X koristi HFS Plus podrazumevano a iOS koristi HFSX.

HFS Plus fajl sistem je nastao iz razloga da se prilagodi skladištenju velikih skupova podataka. Memorija u HFS fajl sistemu je predstavljena pomoću volumena. Oni su podeljeni u sektore od 512 bajtova. Ovi blokovi su grupisani zajedno u alokacione blokove. Njihov broj zavisi od ukupne veličine volumena. HFS Plus koristi adrese blokova od 32 bita za adresiranje blokova alokacije. HFS Plus fajl sistem omogućava efikasno korišćenje prostora na disku, Unicode podršku za imena datoteka, vođenje evidencije o transakcijama, dinamičke promene veličine i mogućnost pokretanja na operativnim sistemima koji nemaju Mac OS.

HFS Plus volumen sadrži više internih struktura kako bi rukovodio organizacijom podataka. Struktura volumena je prikazana na slici 3.



Slika 3. *HFS Plus struktura volumena [2]*

Fajl sistem je podrazumevano konfigurisan kao dve logičke particije diska:

- Sistemska particija podataka – root ili firmware
- Korisnička particija podataka

Sistemska particija sadrži operativni sistem i sve unapred učitane aplikacije koje se koriste sa iPhone-om. Ona je napravljena samo za čitanje. Korisnička particija sadrži sve korisnički kreirane podatke i ona zauzima najveći deo NAND memorije. Najviše podataka se može naći na ovoj particiji.

4.3. iOS sigurnost

Apple iOS uređaji su dizajnirani sa više slojeva sigurnosti. Hardverske funkcije niskog nivoa štite od napada malware-dok funkcije visokog nivoa operativnog sistema sprečavaju neovlašćenu upotrebu.

Pod iOS sigurnosne slojeve se ubrajaju: lozinka, code signing, sandboxing, enkripcija, zaštita podataka, address space layout randomization, odvajanje privilegija, stack smashing protection, data execution prevention, brisanje podataka, aktiviranje zaključavanja.

4.4. Jailbreaking

Pored svih pomenutih zaštita i sigurnosti koje iOS pruža, danas postoji jedan proces koji ih zaobilazi a to je jailbreaking. On uz pomoć eksploatacije softvera i hardvera skida postavljena ograničenja od strane Apple mobilnog operativnog sistema. On dozvoljava izvršavanje nepotpisanog koda i dobijanje root pristupa na operativnom sistemu. Jailbreaking može pomoći u forenzičkoj akviziciji ali će poništiti garanciju koju korisnik ima, može „slomiti“ telefon i može da ne podrži vraćanje na fabrička podešavanja.

Skoro sve verzije iOS-a se mogu jailbreak-ovati.

5. AKVIZICIJA PODATAKA IZ iOS UREĐAJA

Postoje mnogi forenzički alati i metode koje zahtevaju da se uređaj nalazi u jednom od sledećih režima rada – normalni režim, režim oporavka i DFU režim, kako bi se akvizicija uspešno izvršila.

Normalni režim rada - Kada je iPhone uključen, butovan je normalan režim. U ovom modu mogu se izvršavati najregularnije aktivnosti (dopisivanje, razgovor, itd).

Režim oporavka - Tokom boot-up procesa, ukoliko jedan od koraka ne može da se ispuni (da se učita i verifikuje naredni), boot-up proces se zaustavlja i na iPhone-u se prikazuje crni ekran sa jasnom slikom da treba izvršiti povezivanje iPhone i iTunes-a USB kablom. Ovaj režim je režim oporavka i on se koristi prilikom nadogradnje uređaja ili za reinstalaciju uređaja.

DFU režim - Tokom boot-up procesa, ukoliko Boot ROM nije u mogućnosti da verifikuje LLB, onda se na iPhone-u prikaže crni ekran. Ovaj režim je poznat kao Device Firmware Upgrade (DFU). Ovaj režim je režim niskog nivoa i dizajniran je za izvršavanje firmware nadogradnja za iPhone.

Za fizičku akviziciju podataka iOS uređaja biće objašnjene dve metode – akvizicija pomoću prilagođenog diska i preuzimanje slike sistemske korisničke particije.

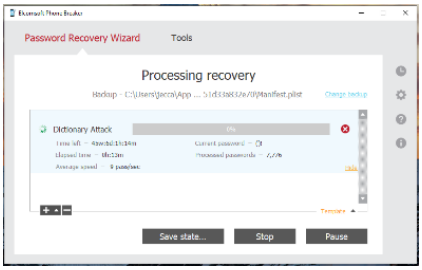
Akvizicija pomoću prilagođenog diska podrazumeva iskorišćavanje slabosti u boot procesu dok je uređaj u DFU režimu tako što se učita prilagođen disk i preko njega se dobije pristup fajl sistemu. Prilagođen disk sadrži forenzičke alate potrebne za kopiranje fajl sistema preko USB-a kroz SSH tunel.

Kako se iOS uređaj sastoji od dve particije, sistemske i korisničke, cilj **akvizicije podataka preuzimanjem slike sistemske korisničke particije** je da se se izvuku svi podaci sa ovih particija. Kompletna forenzička analiza podrazumeva da su preuzeti podaci sa obe particije. Većina forenzičkih alata preuzima sliku obe particije zajedno.

Akvizicija podataka uz pomoć iOS rezervnih kopija je veoma korisna kada fizička, fajl sistem ili logička ekstrakcija iOS uređaja nije moguća. U takvim situacijma, ispitivači kreiraju rezervnu kopiju uređaja i analiziraju je koristeći određeni forenzički alat. Sam proces kreiranja rezervne kopije se vrši na iPhone-u, dok se pomoću USB-a te kopije strimuju na kompjuter. Rezervne kopije mogu enkriptovane. Enkriptovane rezervne kopije sadrže par dodatnih podatka koje obična rezervna kopija nema.

5.1. Elcomsoft Phone Breaker alat

Elcomsoft Phone Breaker je komercijalni alat napravljen od strane Elcomsoft kompanije za Windows platformu. Ovaj alat može dekriptovati enkriptovane rezervne kopije kada lozinka nije dostupna. Obezbeđuje opciju brute-force ili dictionary napada (slika 4) za otkrivanje lozinke.



Slika 4. *Izvršavanje dictionary napada*

Lozinke koje su kratke i jednostavne, mogu biti pronađene u razumnom vremenu. Ukoliko je je lozinka jaka i kompleksna, pronalazak može trajati dosta dugo.

6. ZAKLJUČAK

Mobilni uređaji su nezaobilazno sredstvo u svakodnevnom životu pojedinaca. Namenjeni za komunikaciju i korišćenje raznih servisa, sa sobom nose mnoštvo podataka o korisnicima. Kao takvi postaju glavna meta raznih zloupotreba i kriminalnih aktivnosti zbog podataka kojima su pohranjeni.

U ovom radu je obrađena tematika digitalne forenzike mobilnih uređaja sa akcentom na iOS koja je jedna od najzastupnjenijih platformi.

Digitalna forenzika, konkretnno forenzika iOS uređaja je značajna i jedna je od brzo rastućih grana. Svakodnevno se usavršava i prati trendove koje joj novi modeli uređaja nameću. Neosporno je da će, u budućnosti, biti jedna od najrazvijenijih grana digitalne forenzike.

7. LITERATURA

[1] Milana M. Pisarić, Posebnosti dokazivanja dela visokotehnološkog kriminala, Univerzitet u Beogradu, Pravni fakultet, Beograd, 2016. [Online] Dostupno: https://uvidok.rcub.bg.ac.rs/bitstream/handle/123456789/1097/Doktorat.pdf?sequence=1 (pristupljeno u avgustu 2020.)

[2] Arnes André, Digital forensics: an academic introduction. Hoboken, NJ: John Wiley & Sons Inc., 2018.

[3] ROHIT TAMMA, HEATHER MAHALIK AND SATISH BOMMISETTY, Practical Mobile Forensics - Second Edition, Packt; May 2016

[4] Milorad S. Markagić, Forenzika mobilnih uređaja, 2013, pp.123-135,. [Online] Dostupno: https://cyberleninka.ru/article/n/forenzika-mobilnih-ure-aja/viewer (pristupljeno u septembru 2020.)

[5] Predrag Alargić, Tanja Kaurin, Digitalna forenzika mobilnih uređaja korišćenjem JTAG interfejsa, 2013. [Online] Dostupno: https://infoteh.etf.ues.rs.ba/zbornik/2013/radovi/RSS-8/RSS-8-6.pdf (pristupljeno u avgustu 2020.)

[6] Istraživanje globalnog indeksa o konkurentnosti Svetskog ekonomskog foruma (WEF) za 2019. godinu; https://www.weforum.org/ (pristupljeno u avgustu 2020.)

Kratka biografija:

Jelena Maravić je rođena 16. jula 1996. godine u Subotici. Završila je osnovnu školu „Kizur Ištvan“ u Subotici, a zatim je upisala opšti smer – Ekonomski tehničar u srednjoj ekonomskoj školi „Bosa Milićević“ u Subotici. Godine 2014. osvaja prvo mesto na Republičkom takmičenju ekonomskih srednjih škola iz matematike. Školske 2015/2016. godine upisuje Fakultet tehničkih nauka u Novom Sadu, na studijskom programu Softversko inženjerstvo i informacione tehnologije. Diplomirala je 2019. godine sa temom „Softverski paket za podršku rada sistema bioskopa“. Master studije je upisala iste godine, na istom odseku, modul Elektronsko poslovanje.