Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.42:004.738.12
DOI: https://doi.org/10.24867/15BE14Trifkovic

KOMPARATIVNA ANALIZA OPEN-SOURCE ALATA ZA DIGITALNU FORENZIKU MOBILNIH UREĐAJA

COMPARATIVE ANALYSIS OF OPEN-SOURCE MOBILE DEVICE DIGITAL FORENSICS TOOLS

Bojan Trifković, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTRONSKO POSLOVANJE

Kratak sadržaj – *Rad se bavi komparativnom analizom nekoliko besplatnih alata namenjenih za digitalnu forenziku mobilnih uređaja. Sadržaj je baziran na pojašnjenju osnovnih pojmova digitalne forenzike kao i opisa načina rada uz pomoć ovih alata.*

Ključne reči: *digitalna forenzika, mobilni uređaji, otvoreni kod, Deft, Santoku, Autopsy*

Abstract – *The paper deals with the presentation of open-source tools for digital forensics of mobile devices, with a part dedicated to digital forensics itself as a technological discipline. The paper describes how to use certain tools, as well as their advantages and disadvantages.*

Keywords: *digital forensics, mobile devices, , open-source, Deft, Santoku, Autopsy*

1. UVOD

Forenzika je nauka ili naučna disciplina koja se koristi u krivično pravnom sistemu [1].

Kompjuterska forenzika je posebna oblast forenzike, koja podrazumeva prikupljanje, analizu i ispitivanje podataka u cilju korišćenja istih kao dokaznog materijala protiv osumnjičenih ili u istragama [1].

Digitalna forenzika je nauka ili proces kroz koji se digitalni dokazi iz kompjutera, kamera, fotoaparata, memorijskih uređaja i slično, identifikuju, oporavljaju, čuvaju i prezentuju [1]. Postoji nekoliko vrsta softverskih alata i procesa koji se koriste za sprovođenje uspešne istrage. Među najpoznatije besplatne softverske alate spadaju *Autopsy*, *Deft* i *Santoku*.

Proces digitalne forenzike obezbeđuje istražiteljima uputstvo kako da upravljaju dokazima u toku istrage i kako da reprezentuju nalaze. Bez ovog uputstva dokazi mogu biti izgubljeni odnosno mogu se propustiti neke ključne stavke značajne za istragu [1].

2. FORENZIKA MOBILNIH UREĐAJA

Tokom 2018. godine više od polovine svih *online* aktivnosti pripisano je mobilnim uređajima i taj trend se i dalje nastavlja. Ovo je dovelo do toga da su oni kojima su potrebne razne informacije i cilju istrage ili obaveštajnih pitanja primorani da se obrate ekspertima za forenziku mobilnih uređaja.

2.1. Šta je forenzika mobilnih uređaja

Mobilna forenzika je vrsta digitalne forenzike koja ima za cilj preuzimanje podataka iz mobilnih uređaja, odnosno pametnih telefona i tableta. Mobilni uređaji poseduju razne tipove važnih podataka, počev od istorije poziva i SMS poruka do istorije internet pretraživača i istorije GPS lokacije, koja može dati informacije gde se vlasnik uređaja nalazio u određeno vreme [1].

O forenzici mobilnih uređaja najčešće se razmišlja u kontekstu sprovođenja zakona ali to ne mora da bude uvek tako, danas se i vojska često oslanja na informacije iz mobilnih uređaja prilikom planiranja svojih akcija ili protivterorističkih aktivnosti. Takođe i kompanije mogu ispitivati mobilne uređaje svojih zaposlenih ukoliko sumnjaju da im se krade intelektualno vlasništvo ili je zaposleni uključen u neke nedozvoljene aktivnosti.

2.2. Proces forenzike mobilnih uređaja

Ključ za prikupljanje digitalnih dokaza je poštovanje određenih pravila i praksi tokom tog procesa. Referentni model elektronskog otkrića nastao na Duke univerzitetu definisan je postupcima koji se koriste za prikupljanje elektronskih informacija.

2.3. Koraci u postupku ispitivanja digitalnih dokaza

Postupak ispitivanja digitalnih dokaza uključuje identifikaciju, pripremu, izolaciju, procesuiranje, verifikaciju, dokumentovanje, prezentovanje i čuvanje.

2.4. Mobilni i desktop uređaji u digitalnoj forenzici

Veoma često istražitelji moraju da rukuju istovremeno sa više digitalnih uređaja tokom istrage što znači da način rukovanja u velikoj meri može uticati na ishod istrage. Pored toga određeni operativni sistemi omogućavaju mobilnim i desktop uređajima da lako razmenjuju informacije između dve vrste uređaja. Na primer *Apple MacOS* i *iOS* rade u tandemu kako bi omogućili korisnicima da rad sa desktop uređaja mogu lako da nastave prebacivanjem na mobilni uređaj i obrnuto. Ova mogućnost nazvana "kontinuitet" je primer kako odnos između mobilnih i desktop uređaja može uticati na forenzičarske istrage, što znači da istražitelji mogu da rade na jednom uređaju i lako se po potrebi prebace na drugi. Ono što digitalni forenzičari moraju uvek da pretpostave jeste da napadi mogu biti izvršeni korišćenjem više uređaja od strane jednog hakera ili grupe.

NAPOMENA:

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

2.5. Operativni sistemi mobilnih uređaja

Mobilni operativni sistem je operativni sistem namenjen za mobilne telefone, tablete, pametne satove i druge mobilne uređaje. Putem operativnog sistema mobilni uređaj upravlja svojom memorijom i resursima. Postoji više vrsta operativnih sistema mobilnih uređaja, neki od najpoznatijih operativnih sistema za pametne mobilne uređaje su *Anrodid* i *iOS*. Mobilni uređaji sadrže mnoštvo interfejsa ka spoljašnjem svetu.

Bezbednost ovih interfejsa od različitih napada i neovlašćenog korišćenja je ključna stavka bezbednosti mobilnih telefona danas [1].

Mobilni telefoni imaju mnogo interakcija sa spoljašnjim svetom: Wi-Fi, Bluetooth, SD kartice, USB portovi itd. Takođe, većina korisnika ima pristup bankovnim računima, platnim sistemima banke, poverljivim dokumentima, lozinkama i sličnom u svom telefonu. Ovo ima velike rizike po korisnike telefona.

U cilju zaštite mobilnih uređaja koriste se različiti mehanizmi autentifikacije. Neki od najvećih rizika za mobilne uređaje su: curenje podataka, mešanje poslovnog i privatnog sadržaja i napadi koji su usmereni na ubacivanje *malware* softvera.

2.6. Uobičajeni tipovi podataka u forenzici mobilnih uređaja

Mobilni telefoni sadrže različite tipove podataka koji se mogu prikupiti i analizirati u forenzičkoj istrazi. Najčešće se obraća pažnja na nekoliko mesta na kojima se čuva velika većina podataka, a to su memorija telefona, SIM kartica kao i spoljni uređaji za čuvanje podataka. Digitalni forenzičari se najčešće bave podacima koji se nalaze u memoriji uređaja. Uobičajeni tipovi podataka povezanih sa mobilnim uređajima koji se koriste u istragama su: istorija poziva, kontakti, *SMS* i *MMS* poruke, multimedijalni sadržaj, elektronska pošta, istorija internet pretraživača, podaci aplikacija, istorija lokacije, kalendar, obrisani podaci itd.

Nekim od navedenih podataka se može lako pristupiti (npr. fotografijama, porukama, elektronskoj pošti). Ostalim podacima posebno onim pohranjenim u aplikacijama, može biti teže pristupiti ili mogu biti šifrirani.

2.7. Prikupljanje i analiza dokaza u forenzici mobilnih uređaja

Od istražitelja se očekuje poznavanje industrijskih standarda i najboljih praksi prikupljanja i analize dokaza tako da se prikupljeni podaci mogu iskoristiti i čuvati na sudu. Da bi se dokazi iz mobilnih uređaja mogli proći kontrolu na sudu, postoje određena pravila koja bi dokazi trebalo da ispoštuju: autentičnost, pouzdanost, verodostojnost, temeljnost, prihvatljivost.

Postoje najčešće tri vrste prikupljanja podataka sa mobilnih uređaja: ručno, logičko, fizičko. Najkritičniji aspekt prikupljanja podataka je održavanje integriteta dokaza. Bez obzira koja metoda za pribavljanje se koristi, dokumentovanje tog procesa je ključno za stvaranje dokaza koji su verodostojni i pouzdani.

2.8. Klasifikacioni sistem za forenziku mobilnih uređaja

Klasifikacioni sistem kreiran je sa ciljem kako bi istražiteljima dao pregled dostupnih alata koji se koriste u svrhu prikupljanja dokaza kao i njihov način upotrebe, počev od najmanje kompleksnih pa do onih najsloženijih.

Postoji pet nivoa tehnika za izvlačenje podataka: manuelno, logičko, *hex dump, chip off* i mikro čitanje.

3. ALATI ZA DIGITALNU FORENZIKU MOBILNIH UREĐAJA

Alati za digitalnu forenziku dele se u više kategorija, tako da tačan izbor alata zavisi od potreba i mogućnosti korisnika. Postoji nekoliko kategorija kojima su namenjeni alati: forenzika baza podataka, analiza elektronske pošte, forenzika audio i video sadržaja, analiza internet pretrage, forenzika mreže, forenzika operativne memorije uređaja, analiza fajl sistema, kompjuterska forenzika.

S obzirom na mnoge mogućnosti, nije lako odabrati pravi alat koji će odgovarati potrebama istražitelja. Neki od aspekata koje treba razmotriti tokom donošenja odluke su: nivo veština, izlazni rezultati, budžetska ograničenja, područje fokusa istrage i dodatna oprema.

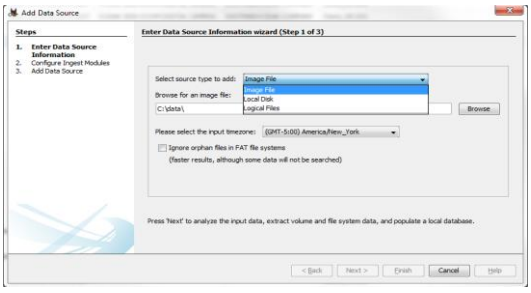
Neki od najpopularnijih besplatnih alata za digitalnu forenziku su [2]: *The Sleuth Kit and Autopsy, SIFT, Deft, Santoku* i *Caine.*

3.1. Autopsy i Sleuth Kit

Autopsy je softverski alat, jednostavan za upotrebu, zasnovan na *GUI* – u, koji omogućava efikasnu analizu diskova i pametnih telefona. Radi na *Windows* operativnom sistemu.

Sleuth Kit je kolekcija command line alata i biblioteka u programskom jeziku C koji omogućavaju analizu diska i vraćanje obrisanih datoteka. Koristi se iza scene u *Autopsy* alatu i mnogim drugim open source i komercijalnim alatima za forenziku.

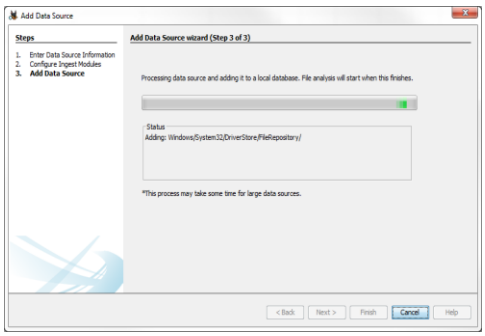
Osnovni koncepti Autopsy alata su: izvor podataka (*data source*), slučaj (*case*) i centralna baza podataka. Na slici 1 prikazan je dijalog prozor gde korisnik bira tip izvora podataka.



Slika 1. *Dijalog prozor za dodavanje izvora podataka*

Na slici 2 prikazan je dijalog prozor gde korisnik prati status osnovnog ispitivanja izvora podataka.

Pre dodavanja izvora podataka korisnik mora da kreira novi slučaj. Autopsy podržava tri vrste izvora podataka: slika diska, lokalni disk i logičke datoteke.



Slika 2. *Dijalog prozor statusa ispitivanja izvora podataka*

Autopsy je softverski alat koji omogućava veoma efikasnu i pouzdanu analizu čvrstih diskova kao i pametnih telefona, tableta i drugih *Androd* uređaja. Karakteriše ga korisnički interfejs koji je veoma intuitivan i lak za upotrebu, brzo procesuiranja podataka i niski troškovi. Sleuth Kit je kolekcija sastavljena od command line alata i biblioteka u programskom jeziku C koji omogućavaju analizu slike diska i oporavak fajlova i podataka. To se zapravo koristi kao pozadina Autopsy alata, odnosno kao njegov backend alat.

3.2. Deft

Deft je distribucija *Linux* operativnog sistema namenjena za digitalnu forenziku. *Deft* se smatra najboljim izborom među bezbedonosnim agencijama i agencijama za sprovođenje zakona za forenzičarske istrage [3]. Slika 3 prikazuje korisnički interfejs ovog operativnog sistema.

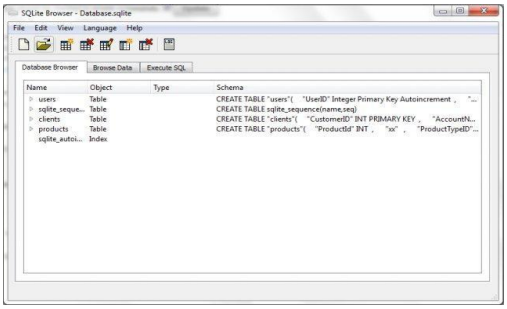
Slika 3. *Izgled Deft operativnog sistema*

Deft sadrži *DART* paket koji sadrži *Windows* aplikacije koje su i dalje održive jer u *Unix* operativnim sistemima ne postoji ekvivalent. Pokretanje *Windows* aplikacija na *Linux* operativnom sistemu u slučaju *Deft* distribucije moguće je uz pomoć softverskog alata koji se naziva *Wine*. *DART* je aplikacija koja organizuje, prikuplja i pokreće softver u sigurnom režimu u svrhu forenzičke analize uživo i reagovanja na bezbednosne incidente.

Deft Linux uključuje i neke alate za analizu mobilnih uređaja. Dostupan je pretraživač *SQLite* baze podataka koji omogućava analizu podataka koji se koriste u većini aplikacija za *Android*, *iPhone* i *iPad* uređaja.

Postoji i *Ipddump* za analizu backup-ova *BlackBerry* uređaja, kao i *iPhone analyzer* za analizu *iPhone* uređaja koji je dostupan od verzije 3 pa na više [4]. S obzirom da *Android* i *iPhone* pametni telefoni većinu podataka čuvaju upravo u *SQLite* bazi podataka, *SQLite database browser* omogućava korisniku uvid u podatke kroz grafički prikaz.

Na slici 4 prikazan korisnički interfejs taba *Database browser* u okviru *SQLite database browser* alata.



Slika 4. *Database browser* tab u okviru *SQLite database browser* alata

Za pretragu fajlova i direktorijuma u okviru *Deft* operativnog sistema može se koristiti softverski alat *Catfish*. *Catfish* može izvoditi iste operacije koje se mogu izvršiti putem naredbi komandne linije *find* i *locate*.

Prednosti *Deft*-a su jako mali memorijski zahtevi za pokretanje aplikacije (svega 400 MB). Ovo znači da može biti pokrenut i na starijim, sporijim računarima.

3.3. Santoku

Santoku Linux je besplatni projekat otvorenog koda sponzorisan od strane kompanije "*NowSecure*" iz Čikaga, čiji članovi čine jezgro razvojnog tima [5]. *Santoku* je napravljen sa ciljem da omogući rad u polju mobilne forenzike i analize bezbednosti i upakovan je u platformu otvorenog koda koja se lako koristi. *Santoku* uključuje veliki broj alata otvorenog koda koji omogućavaju rad sa svim aspektima mobilne forenzike, analize *malware*-a i bezbednosno testiranje. Izgled UI Santoku operativnog sistema prikazan je na slici 5.

Slika 5. *Izgled Santoku operativnog sistema*

Tipovi forenzike podržani od strane *Sandoku* operativnog sistema i njegovih alata su: logička, forenzika fajl sistema i forenzika fizičkih diskova. Logička analiza i pribavljanje podataka vrši se uz pomoć aplikacije *AF Logical OSE* iz menija *Device Forensics*. Rezultat ove analize može dati uvid u razne vrste podataka na telefonu kao što su kontakti, slike, istorija poziva i SMS poruke. Prednosti *Santoku* operativnog sistema su sto je brz za ovu vrstu analize. Forenzika fajl sistema omogućava analizu veće količine podataka nego logička analiza, ali zahteva i dodatni pristup uređaju. Fizička analiza podrazumeva kopiranje bit po bit fizičkog memorijskog uređaja i to je najčešće korišćena forenzička tehnika iz razloga što su najveće šanse za oporavak obrisanih podataka [6].

4. DISKUSIJA

Ovaj rad se bavi analizom tri besplatna alata namenjenih digitalnoj forenzici mobilnih uređaja. Stiče se utisak da razvoj besplatnih alata za forenziku mobilnih uređaja još uvek nije dosegao nivo koji bi omogućio veću zainteresovanost inženjera za njihovo istraživanje, upotrebu ili direktno učestvovanje u razvoju istih.

Autopsy se može smatrati alatom koji je najsličniji komercijalnim alatima za digitalnu forenziku. Razlog ovog mišljenja jeste način upotrebe ovog alata i njegov napredni korisnički interfejs koji omogućava kreiranje vizuelnih i lako čitljivih izveštaja o rezultatima operacija. Za razliku od *Deft* i *Santoku* operativnih sistema koji pored mogućnosti obavljanja operacija digitalne forenzike imaju još dodatnih funkcionalnosti, *Autopsy* je softver primarno namenjen digitalnoj forenzici.

Deft je verzija *Linux* operativnog sistema bazirana na Ubuntu distribuciji koja nudi preko 1GB dodatnog besplatnog softvera. *Deft* poseduje mogućnost pokretanja *Windows* aplikacija uz pomoć alata koji se zovu *LXDE* i *WINE*, dok *Santoku* nema mogućnost rada sa ova dva softvera jer nije baziran na *Ubuntu* distribuciji operativnog sistema.

Deft Linux takođe nudi mogućnost obavljanja forenzičarskih zadataka iz domena pametnih i mobilnih uređaja. *SQLite database browser* omogućava pregled baza podataka *Android* aplikacija u okviru telefona. Nudi mogućnost tabelarnog prikaza kroz intuitivan korisnički interfejs. Korisnički interfejs na visokom nivou omogućava istražiteljima jasan uvid u podatke u okviru aplikacije, što znatno ubrzava i olakšava istrage.

Santoku je *Linux* distribucija čiji je glavni fokus na mobilnoj forenzici, a takođe uključuje alate koji omogućavaju brute force dešifrovanje *Android* uređaja, analiza backup-a *iPphone* uređaja kao i automatsko prepoznavanje priključenih uređaja.

Santoku nudi mogućnost obavljanja tri tipa analize fajlova – logička analiza, forenzika fajl sistema i forenzika fizičkih diskova. Fizička analiza je najpreciznija i najčešće korišćena tehnika analize memorijskih uređaja uz pomoć *Santoku* operativnog sistema, jer podrazumeva kopiranje bit po bit sadržaja memorijskog uređaja te samim tim obezbeđuje velike šanse da se dođe do svih neophodnih podataka. Logička analiza je proces koji takođe iziskuje određeno iskustvo u radu sa *Linux* operativnim sistemom, jer podrazumeva izvršavanje *Linux* komandi u terminalu u toku procesa analize.

Analiza i presretanje mrežnog saobraćaja uz pomoć Santoku Linux operativnog sistema je izuzetno efikasna i uspešna operacija. Od istražitelja koji obavljaju ove zadatke očekuje se određeni nivo predznanja pre svega o mrežnom saobraćaju i *HTTP* protokolu.

Santoku i *Deft* je moguće pokrenuti sa *Windows* operativnog sistema uz pomoć *VMware* i *Virtualbox* softvera (virtuelne mašine). *Autopsy* ne zahteva instalaciju dodatnog operativnog sistema i namenjen je radu na *Windows* operativnom sistemu.

5. ZAKLJUČAK

Digitalna forenzika je oblast koja igra veoma značajnu ulogu u informacionim društvu. Zbog sve veće količine podataka pretpostavke su da će digitalna forenzika imati veoma zapaženu ulogu u budućnosti, jer sa porastom količine podataka raste i rizik od njihove krađe i zloupotrebe.

Trenutno, analizi za digitalnu forenziku mobilnih uređaja otvorenog koda po funkcijama koje nude zaostaju za vlasničkim alatima.

Poslednjih godina primećen je pomak u razvoju alata otvoren koda ka usvajanju i uvođenju novih funkcionalnosti što ih čini pogodnijim i konkurentnijim u budućem radu i korišćenju.

6. BIBLIOGRAFIJA

[1] Computer Science: Mobile Forensics, https://study.com/academy/course/computer-science-335-mobile-forensics.html (pristupljeno u julu 2020.)

[2] Autopsy User Documentation 4.3, https://sleuthkit.org/autopsy/docs/user-docs/4.3/ (pristupljeno u oktobru 2020.)

[3] Forensic Investigation Tutorial Using DEFT, https://www.hackingarticles.in/forensic-investigation-tutorial-using-deft/ (pristupljeno u oktobru 2020.)

[4] DEFT Linux A Linux Distribution For Computer Forensics, http://www.linuxandubuntu.com/home/deft-linux-a-linux-distribution-for-computer-forensics (pristupljeno u martu 2021.)

[5] How to use Santoku in Andorid Forensics?, https://infosecaddicts.com/use-santoku-android-forensics/ (pristupljeno u martu 2021.)

[6] About Santoku, https://santoku-linux.com/about-santoku/ (pristupljeno u aprilu 2021.)

Kratka biografija:

Bojan Trifković rođen je u Petrovu, BiH 1992. god. Master rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Komparativna analiza open-source alata za digitalnu forenziku odbranio je 2021.god.
kontakt: bojantrifkovic92@gmail.com