Forenzika mobilnog uređaja primjenom distribucije Santoku Linux

Karakaš, Toni

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

FORENZIKA MOBILNOG UREĐAJA PRIMJENOM DISTRIBUCIJE SANTOKU LINUX

MOBILE DEVICE FORENSICS BY USING SANTOKU LINUX DISTRIBUTION

Mentor: Doc. dr. sc. Siniša Husnjak

Student: Toni Karakaš

JMBAG: 0023101651

Zagreb, kolovoz 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Forenzička analiza informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6241

Pristupnik: **Toni Karakaš (0023101651)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Forenzika mobilnog uređaja primjenom distribucije Santoku Linux**

Opis zadatka:

Istražiti područje digitalne forenzike. Pojasniti ekstrakcije podataka mobilnih uređaja. Protumačiti Santoku Linux distribuciju za forenzičku analizu mobilnih uređaja. Izvijestiti o funkcionalnostima alata Santoku Linux distribucije. Provesti forenzičku analizu mobilnog uređaja.

Mentor:

doc. dr. sc. Siniša Husnjak

Predsjednik povjerenstva za diplomski ispit:

SAŽETAK

Mobilni uređaji u svakodnevnoj su upotrebi u svim područjima ljudskog života. Upravo iz tog razloga većina bitnih informacija i podataka se prenosi primjenom mobilnih uređaja. Područje forenzičke analize mobilnih uređaja vrlo je važno za otkrivanje kriminalnih aktivnosti u određenim sudskim procesima. Postoje razne metode ekstrakcije podataka sa mobilnih uređaja te je u pravilu kompleksnijom metodom moguće ekstrahirati više podataka. U ovom radu opisana je Santoku Linux distribucija koja sadrži određene alate za logičku ekstrakciju podataka te razne druge alate koji se koriste u području forenzičke analize, penetracijskog testiranja te analize mobilnog zlonamjernog softvera. Cilj ovog diplomskog rada je prikazati metode i načine ekstrakcije podataka te određene Linux distribucije koje se primjenjuju za forenzičku analizu mobilnih uređaja. Nadalje, detaljnije opisati Santoku Linux distribuciju, njene prednosti, nedostatke te sam postupak provedbe forenzičke analize i upotrebu alata za forenziku mobilnih uređaja.

KLJUČNE RIJEČI: forenzička analiza, mobilni uređaj, ekstrakcija podataka, digitalna forenzika

SUMMARY

Mobile devices are in daily use in all areas of human life. The most important information and data is transmitted through mobile devices. The field of forensic analysis of mobile devices is very important for the detection of criminal activities in certain court proceedings. There are various methods of extracting data from mobile devices, and the more complex the method, the more data can be extracted. This thesis describes the Santoku Linux distribution, which contains certain tools for logical data extraction and various other tools used in the field of forensic analysis, penetration testing and mobile malware analysis. The aim of this thesis is to get acquainted with the methods and ways of data extraction and certain Linux distributions that are used for forensic analysis of mobile devices. In particular, describe in more detail the Santoku Linux distribution, its advantages and disadvantages, and the process of conducting forensic analysis and the use of tools for mobile device forensics.

KEY WORDS: forensic analysis, mobile device, data extraction, digital forensics

SADRŽAJ

1. UVOD

Digitalni uređaji u svakodnevnoj su upotrebi, u svim životnim područjima, stoga kontinuirano raste i njihov broj. Samim time, većina privatnih i poslovnih informacija razmjenjuje se upravo putem digitalnih uređaja, naročito kada govorimo o mobilnim uređajima. Upotreba mobilnih uređaja pojednostavila je svakodnevnu komunikaciju u privatnom i poslovnom okruženju, ali isto tako i potaknula razvoj ilegalnih aktivnosti poput krađe podataka i slično. Nadalje, zloupotreba mobilnih uređaja može se povezati i s raznim kriminalnim aktivnostima. Upravo iz navedenih razloga sve veći naglasak stavlja se na područje forenzike mobilnih uređaja, odnosno kontinuirano se razvijaju alati kojima se provode razni oblici ekstrakcije podataka. Forenzika mobilnih uređaja podrazumijeva prikupljanje i ekstrakciju podataka te analizu ekstrahiranih podataka. Svaki digitalni dokaz mora biti prikupljen na legalan način kako bi bio upotrebljiv u mogućim sudskim procesima.

U ovom diplomskom radu opisat će se funkcionalnosti i upotreba Santoku Linux distribucije za forenziku mobilnog uređaja. Navest će se i opisati svi alati koje navedena distribucija sadrži te mogućnosti primjene istih.

Cilj ovog diplomskog rada je opisati i provesti forenziku mobilnog uređaja pomoću Santoku Linux distribucije te ukazati na sve prednosti i nedostatke pojedinih alata koji će se upotrebljavati. Diplomski rad sastoji se od 7 cjelina:

1. Uvod
2. Digitalna forenzika
3. Ekstrakcija podataka mobilnih uređaja
4. Santoku Linux distribucija za forenzičku analizu mobilnih uređaja
5. Funkcionalnosti alata Santoku Linux distribucije
6. Provedba forenzičke analize mobilnog uređaja
7. Zaključak

Drugo poglavlje orijentirano je na definiranje pojmova digitalne forenzike. Navedena je primjena i značaj digitalne forenzike, zatim se detaljnije govori o forenzici mobilnih

uređaja. Prikazana je referentna metodologija forenzike mobilnih uređaja te se opisuju određeni hardverski i softverski orijentirani alati.

U trećem poglavlju detaljnije su opisane vrste ekstrakcije podataka s mobilnih uređaja počevši od najjednostavnijih metoda prema složenijim.

Četvrto poglavlje govori o Linux distribucijama za forenziku mobilnih uređaja, s naglaskom na Santoku Linux distribuciju koja je tema diplomskog rada. Opisane su njene mogućnosti i primjena te alati koje sadrži po područjima primjene.

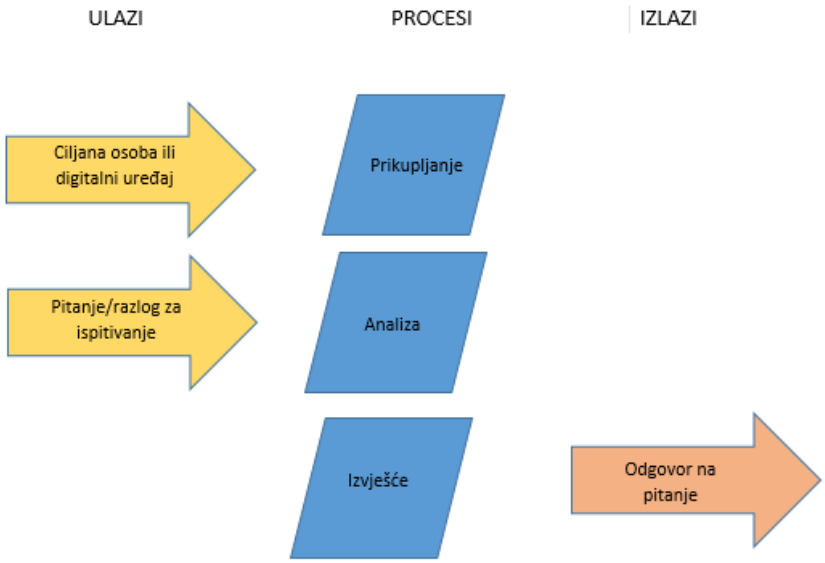
Funkcionalnosti alata unutar Santoku Linux distribucije opisane su u petom poglavlju. Nadalje, navedene su kategorizacije Santoku Linux alata prema područjima primjene.

U zadnjem poglavlju ovog rada prikazana je provedba forenzičke analize mobilnog uređaja pomoću Santoku Linux distribucije. Cilj provedbe forenzičke analize je doći do zaključka o tome koliko su alati unutar Santoku Linuxa korisni za provedbu forenzičke analize.

2. DIGITALNA FORENZIKA

Digitalna forenzika može se definirati kao znanost kojom se provodi ispitivanje digitalnog prostora i digitalnog okruženja s ciljem detektiranja određenih događaja te prikupljanja digitalnih dokaza. Provođenjem forenzičke istrage utvrđuju se trenutna ili prošla događanja u određenom digitalnom uređaju. Digitalna forenzika koristi se za pronalazak digitalnih tragova koji su zapisani prilikom prijašnjih radnji. Isto tako može se koristiti i za stvarno vremensko nadgledanje mrežnog prometa, računalnih i drugih digitalnih sustava. Ovakav oblik forenzike podrazumijeva prikupljanje podataka, analiziranje podataka i izvještavanje o digitalnim podacima.

Forenzička istraga provodi se uz unaprijed određeni cilj istrage ili uz poznate potencijalne okrivljenike, kako bi se pravovremeno mogli prepoznati ključni digitalni dokazi koji su od velikog značaja za forenzičku istragu. Na slici 1 prikazan je općeniti pregled forenzičke istrage koji se sastoji od ulaznih podataka, procesa i izlaznih podataka. Pomoću elemenata sa slike 1 generalno možemo prikazati bilo koji oblik digitalne forenzike.



Slika 1. Općeniti pregled forenzičke istrage

Izvor: [1]

Ulaznim podacima smatraju se ciljane osobe i digitalni uređaji za koje postoje određeni razlozi za provođenje forenzičke istrage. Procesi koje sadrži digitalna forenzika su: prikupljanje podataka, analiziranje podataka i izvještavanje o provedenoj forenzičkoj analizi. Proces prikupljanja podrazumijeva prikupljanje podataka na legalan i dozvoljen način od osumnjičene osobe sa ciljanog digitalnog uređaja. Također, prilikom prikupljanja podataka važno je definirati razlog prikupljanja istih kako bi istražitelji znali koji su ključni dokazi za njihovu daljnju forenzičku istragu. Proces analiziranja podrazumijeva prepoznavanje značaja i važnosti prikupljenih podataka za daljnji proces forenzičke istrage. Izvještavanjem se iznose doneseni zaključci nakon provedenih faza prikupljanja i analiziranja podataka. Vrlo je važno da se prilikom provođenja svih koraka digitalne forenzike poštuju pravila i zakoni lokalnog zakonodavstva, [1].

2.1. Primjena i značaj digitalne forenzike

Područje digitalne forenzike vrlo je bitno u današnjem svijetu zbog toga što se većina komunikacija odvija putem digitalnih uređaja i digitalnih sustava. Kriminalne aktivnosti dogovaraju se i provode putem računala ili mobilnih uređaja te samim time svaki takav uređaj postaje predmetom forenzičke istrage. Digitalna forenzika može se primjenjivati za kriminalističke istrage vezane za ubojstva, trgovanja drogom i ljudima, terorizam, dječju pornografiju i slično. Također, može se primjenjivati za istraživanje napada na sustave javnog sektora ili vlade, obavještajne i protuobavještajne djelatnosti, razne oblike sudskih istraga, korporativnih istraga vezanih za krađu podataka, napade na računalne sustave te za mnoge druge primjene.

Digitalnu forenziku općenito možemo klasificirati na sljedeći način, [2]:

- računalna forenzika
- forenzika mobilnih uređaja
- mrežna forenzika
- forenzika baza podataka
- ostali oblici forenzike.

Ostali oblici forenzike podrazumijevaju *Cloud* forenziku, e-mail forenziku, forenziku IoT uređaja, forenziku podataka, forenziku dokumenata, forenziku društvenih mreža, web forenziku i sve ostale oblike digitalne forenzike.

Digitalna forenzika ima veliki značaj u otkrivanju određenih kriminalnih aktivnosti koje se dogovaraju ili provode putem digitalnih sustava i uređaja. Samim time, forenzičke istrage koje se provode nad takvim uređajima od velikog su značaja za prikupljanje digitalnih dokaza. Prikupljeni digitalni dokazi mogu uputiti na otkrivanje kriminalne aktivnosti ili na otkrivanje osobe koja je počinitelj ilegalne aktivnosti. Forenzičkom istragom dolazi se do poveznice između korisnika uređaja i njihovih aktivnosti na mreži. No, nije uvijek tako jednostavno doći do ključnog digitalnog dokaza. Primjerice, ako logovi pokazuju da se ilegalna aktivnost izvršila preko određenog korisničkog računa, to ne mora značiti da je vlasnik korisničkog računa izvršitelj te aktivnosti, već izvršitelj te aktivnosti može biti napadač koji je kompromitirao navedeni korisnički račun. Upotreba dokaza iz više neovisnih izvora važna je kako bi se dobio bolji uvid u događaj te kako bi se stvorila čvrsta povezanost između pojedinca i računalnih aktivnosti. Dokazivanje određenih radnji teže je ostvariti u slučaju da se počinitelj ilegalne aktivnosti koristi otvorenim bežičnim pristupnim točkama ili javno dostupnim računalima i sličnim uređajima. Mogu se koristiti različiti oblici zavaravanja poput lažnih ili skrivenih IP adresa uređaja pomoću kojih napadači prikazuju da su povezani na mrežu sa posve druge lokacije. Također, istražitelji mogu analizirati metapodatke kojima mogu doći do određenih informacija o tome jesu li određeni dokumenti ili fotografije kreirani na uređaju koji je predmet istrage ili su preuzeti sa Interneta i slično. Ovakav način forenzike metapodataka često se koristi kod forenzičkih istraga vezanih za dječju pornografiju gdje je važno identificirati uređaj i model kamere kojim je fotografija snimljena, [3].

Forenzički istražitelji prilikom prikupljanja dokaza iste moraju prikupljati na legalan način te prikazati njihovo podrijetlo. Navedeno je važno provoditi uz poštivanje svih zakona jer se bilo kakav oblik dokaza prikupljenih na ilegalan način ne priznaje u mogućim sudskim procesima. Područje primjene digitalne forenzike vrlo je široko, stoga zahtijeva široko znanje istražitelja i poznavanje raznih metoda te načina istrage.

2.2. Forenzika mobilnih uređaja

Broj korisnika mobilnih uređaja u kontinuiranom je rastu te prema izvoru [4] procjenjuje se da je u 2020. godini broj korisnika mobilnih uređaja iznosio 6,95 milijardi. Prognoze predviđaju daljnji rast na 7,1 milijardi korisnika do kraja 2021. godine. Navedene brojke dokazuju raširenost primjene mobilnih uređaja u svijetu. Iz tog razloga mobilni uređaji imaju veliku važnost u području digitalne forenzike pa se forenzika mobilnih uređaja vrlo često primjenjuje u svakodnevnici za prikupljanje raznih digitalnih dokaza. Nadalje, mobilni uređaji mogu biti korišteni kao sredstvo dogovaranja ilegalnih aktivnosti, ali isto tako mogu biti korišteni kao sredstvo provođenja istih. U oba slučaja mobilni uređaji sadrže značajne digitalne dokaze za postupak istrage.

Mobilnu forenziku možemo definirati kao skup znanstvenih metodologija sa ciljem ekstrakcije digitalnih dokaza legalnim putem. Ekstrakcija digitalnih dokaza obuhvaća postupke prikupljanja, oporavka i analiziranja podataka koji su pohranjeni na mobilnim uređajima. Ekstrakcija podataka može se provoditi sa interne i eksterne memorije mobilnog uređaja. Kontinuiranim razvojem tehnologije i pametnih mobilnih uređaja povećava se količina digitalnih dokaza, a ujedno i količina podataka koja se treba ekstrahirati i analizirati. Upravo zbog toga, razvojem tehnologije razvijaju se i razne metode provođenja forenzičke analize mobilnih uređaja. Tržište mobilnih uređaja postaje sve veće, a samim time postupak forenzičke istrage postaje složeniji zbog otežanog izbora odgovarajućeg alata kojim će se vršiti prikupljanje podataka i forenzička analiza. Odabir ispravnog pristupa forenzičkoj istrazi, odnosno odabir odgovarajuće metode prikupljanja te analiziranja podataka ključan je za ekstrakciju i pronalazak željenih digitalnih dokaza, [5].

Osim odabira odgovarajućih metoda forenzičke istrage važno je odabrati odgovarajuće hardverske ili softverske alate kojima će se provoditi forenzička istraga. Vrlo često bit će potrebna kombinacija više alata kako bi se prikupili željeni podaci i ostvario željeni rezultat istrage. Na složenost procesa prikupljanja podataka utječu raznolikosti proizvođača i modela mobilnih uređaja, različiti operativni sustavi, različite sigurnosne značajke uređaja te tehnike antiforenzike. Nadalje, tehnikama antiforenzike skrivaju se ili brišu podaci kako bi se otežalo njihovo prikupljanje i pronalaženje. Osim navedenih razloga, provedbu istrage mogu otežati

pravna pitanja i zakoni, programi sa zlonamjernim kodom, alati koji ne podržavaju sve modele mobilnih uređaja i slično, [5].

2.2.1. Referentna metodologija forenzike mobilnih uređaja

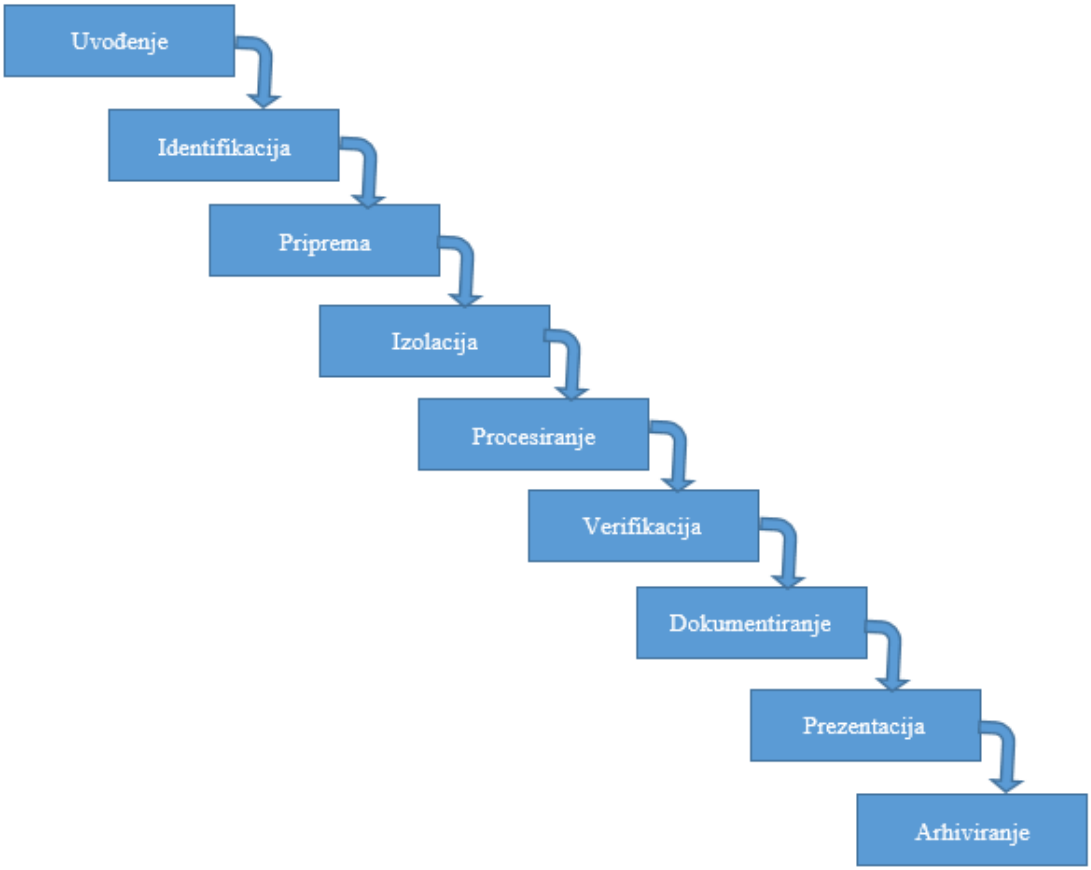
Postoji velik broj različitih metodologija forenzike mobilnih uređaja. Svaka metodologija mora se pridržavati principa digitalne forenzike. Principi digitalne forenzike definiraju da niti jedna aktivnost ne smije izmijeniti podatke koji su predmet forenzičke istrage. Također, samo u iznimnim slučajevima dopuštena je forenzička analiza na originalnim podacima kako bi se smanjila mogućnost gubitka ili oštećenja istih. Cijeli proces forenzičke istrage i analize mora biti pravilno dokumentiran kako bi sam proces istrage bio legalan i prihvatljiv za moguće sudske procese. Prilikom provođenja forenzičke istrage, forenzički istražitelji moraju se pridržavati svih propisa i zakona tijekom procesa prikupljanja i analize podataka.

NIST metodologija jedna je od poznatijih metodologija forenzike mobilnih uređaja. *The National Institute of Standards and Technology* (NIST) predstavlja specijaliziranu ustanovu Ministarstva trgovine Sjedinjenih američkih država koja ima za cilj promovirati inovacije i industrijsku kompetitivnost. Uključuje znanost, informacijsku tehnologiju, mjerenje materijala i slično. Prema izvoru [6] iz 2014. godine NIST-ova metodologija sastoji se od sljedećih faza:

- očuvanje dokaza
- prikupljanje podataka
- ispitivanje i analiza
- izvještavanje.

NIST-ova metodologija jedna je od poznatijih, no kao referentna metodologija forenzike mobilnih uređaja smatra se metodologija definirana od strane istražiteljice Cynthie A. Murphy koja je radila na SANS institutu. SANS je privatna profitna tvrtka specijalizirana za područje informacijske i kibernetičke sigurnosti te za prodaju certifikata. Prema izvoru [7] čiji je autor ranije spomenuta istražiteljica, referentna metodologija forenzike mobilnih

uređaja može se prikazati u devet faza. Navedene faze referentne metodologije prikazane su na slici 2.



Slika 2. Referentna metodologija forenzike mobilnih uređaja

Izvor: [7]

Uvođenje predstavlja prvu fazu metodologije mobilne forenzike prikazane na slici 2. Navedena faza podrazumijeva pripremu dokumentacije kao što je lanac posjeda dokaza, informacije o vlasniku, tipu incidenta, modelu mobilnog uređaja, tipu podataka koji će se prikupljati i ostalu dokumentaciju o početku istraživačkog procesa. Vrlo često u ovoj fazi koristi se i određeni obrazac za unos informacija o istraživanju.

Identifikacija svakog mobilnog uređaja podrazumijeva pravnu punomoć za provođenje procesa forenzičke istrage, ciljeve istraživanja, identificiranje modela i informacija, identificiranje uklonjive i eksterne pohrane te potencijalne druge izvore dokaza.

Priprema obuhvaća određivanje dostupnih alata koji su kompatibilni za određeni model mobilnog uređaja kako bi se uspješno izvršila ekstrakcija željenih podataka. U prethodnoj fazi identifikacije već se izvršila određena priprema za forenzičku istragu, tako da se ova faza više bazira na odabir konkretnih alata i načina ekstrakcije podataka za postizanje definiranog cilja istrage.

Izolacija mobilnog uređaja vrlo je važna zbog toga što se tako sprječava izmjena postojećih te dodavanje novih podataka na uređaj. Iz tog razloga, mobilni uređaj mora se izolirati od povezanosti sa svim komunikacijskim mrežama kao što su internetska mreža, Wi-Fi, Bluetooth, mobilna mreža i slično. Na taj način onemogućeno je uspostavljanje novih poziva, slanje poruka te presnimavanje drugih podataka preko postojećih. Također, izolacijom se onemogućuje udaljeni pristup mobilnom uređaju te brisanje podataka udaljenim pristupom.

Procesiranje uklonjivih medija za pohranu podataka mora se vršiti odvojeno od procesiranja podataka mobilnog uređaja ukoliko je to moguće. Razlog tome je što istraživanje podataka na mobilnom uređaju može utjecati na podatke na vanjskom mediju za pohranu podataka. Navedeno nije moguće ukoliko su podaci kriptirani te ih je u tom slučaju moguće čitati jedino s uređaja. Korištenje više metoda i načina ekstrakcije korisno je u smislu dekodiranja prikupljenih podataka sa mobilnog uređaja.

Faza verifikacije podrazumijeva provjeru točnosti podataka ekstrahiranih sa uređaja. Ponekad se pojavljuju pogreške u prikazivanju ekstrahiranih podataka, koje nastaju greškom u radu odabranih alata za prikupljanje podataka sa uređaja. Verifikacija se može izvršiti na nekoliko načina. Jedan od načina je usporedba ekstrahiranih podataka sa podacima na mobilnom uređaju te ispitivanje njihove podudarnosti. Ostali načini verifikacije podrazumijevaju uporabu više različitih alata te uspoređivanje dobivenih rezultata, provjerom *hash* vrijednosti podataka i slično.

Dokumentaciju je potrebno voditi tijekom cijelog procesa planiranja i provođenja forenzičke istrage mobilnog uređaja. Važno je voditi lanac posjeda dokaza kako bi dokazi bili

prikupljeni na legalan način te bili primjenjivi u mogućim sudskim procesima. Dokumentacija sadrži podatke o početku istraživanja, fizičkom stanju mobilnog uređaja, slike uređaja nad kojim se provodi forenzička istraga, podatke o proizvođaču i modelu uređaja, korištene alate tijekom istrage i slično.

Prezentacija obuhvaća jasno i razumljivo prikazivanje dobivenih rezultata istrage drugim forenzičarima, tužiteljima i sudu. Mora sadržavati konkretne dokaze i informacije, a sadržaj mora biti objašnjen i prilagođen publici kojoj je namijenjen.

Arhiviranje podrazumijeva očuvanje ekstrahiranih i dokumentiranih podataka te je važan dio cjelokupnog procesa forenzičke analize mobilnih uređaja. Nužno je očuvati ekstrahirane podatke u upotrebljivom formatu kako bi se isti mogli iskoristiti u mogućim sudskim procesima, kao buduća referenca ili za potrebe vođenja evidencije. Određene forenzičke istrage mogu se odužiti, zbog čega je ova faza vrlo važna u cjelokupnoj metodologiji forenzike mobilnih uređaja. Poželjno je ekstrahirane podatke spremiti na standardne medije za pohranu u vlasničkom i nevlasničkom formatu kako bi kasnije bili dostupni po potrebi. Isto tako poželjno je napraviti kopiju korištenog alata kako bi se olakšao kasniji pregled ekstrahiranih podataka, [7].

2.2.2. Digitalni dokazi mobilnih uređaja

Digitalne dokaze možemo definirati kao bilo koju vrstu digitalnih podataka koja sadrži pouzdane i točne informacije koje mogu potvrditi ili opovrgnuti postavljenu hipotezu istraživanog incidenta ili zločina. Važno je voditi lanac posjeda dokaza kako bi se svi digitalni dokazi dokumentirali i pohranili na ispravan način. Metapodaci, odnosno podaci o podacima, jedna su od značajnijih vrsta digitalnih dokaza koja sadrži informacije o podatkovnim objektima. Primjerice, metapodaci koji su vezani za fotografiju mogu biti datum i vrijeme snimanja fotografije, lokacija snimanja fotografije te model kamere koji je upotrijebljen. Upravo zbog navedenog, metapodaci su vrlo važni kao digitalan dokaz u svim procesima forenzičke istrage mobilnih uređaja budući da često sadrže ključne informacije za rješavanje slučajeva i istraga, [8].

Digitalni dokazi prisutni su na svakom digitalnom uređaju jer svaka radnja na takvom uređaju ostaje zapisana. Postoje razni podaci koji u određenim slučajevima imaju dokaznu vrijednost. Digitalnim dokazima možemo smatrati razne datoteke, baze podataka, adresar, e-poštu te razne dinamičke podatke poput log zapisa, *history* datoteke, kolačića itd.

2.2.3. Hardverski orijentirani alati za forenziku mobilnih uređaja

Tvrtka *Cellebrite* smatra se jednom od najpopularnijih tvrtki u području forenzike mobilnih terminalnih uređaja. Razvija hardverske i softverske alate za provođenje forenzičke analize mobilnog uređaja. *Cellebrite* je razvio hardverske alate poput *UFED Touch, UFED 4PC, UFED TK, UFED Infield Kiosk, UFED Chinex.*

UFED Touch2 je prijenosna hardverska platforma za digitalnu forenziku koja omogućava rad u laboratoriju, sa udaljenog mjesta ili na terenu. Nadalje, *UFED Touch2* omogućava brzo prikupljanje podataka unutar zatvorenog okruženja kako bi se izbjegao svaki rizik utjecaja na prikupljene digitalne dokaze. Može prikupljati slike, video zapise, logove poziva i bilo koji drugi oblik logičkih podataka sa mobilnih uređaja. Ima produženi vijek trajanja baterije te se prikupljenim podacima odmah može pristupiti. Postoji i *UFED Touch2 Ruggedized* verzija koja je dodatno zaštićena kako bi omogućila rad u najtežim terenskim uvjetima. Na slici 3 prikazana je *UFED Touch2 Ruggedized* verzija modela.

Slika 3. *UFED Touch2 Ruggedized,* [9]

UFED Ruggedized Laptop je proizvod tvrtke *Cellebrite* koji na malom prijenosnom računalu omogućava prikupljanje podataka te može podnijeti ekstremne temperature, padanja,

vibracije i većinu ostalih elemenata koji mogu biti prisutni u terenskom radu. Laptop dolazi u dobro zaštićenoj kutiji namijenjenoj terenskim uvjetima.

UFED Kiosk omogućava brzo prikupljanje podataka i analizu na određenim mjestima kao što su granični prijelazi ili policijske postaje. Ovakvo samostalno hardversko rješenje nudi sigurnu i zatvorenu hardversku platformu koja omogućava brzo djelovanje istražiteljima. Na slici 4 prikazan je *UFED Kiosk,* [9].

Slika 4. *UFED Kiosk,* [9]

Osim Cellebrite hardverskih platformi, također i MSAB je razvio različite hardverske platforme kao što su *MSAB Office* koji je namijenjen za digitalnu forenziku u laboratorijima. Također, postoji i terenska verzija *MSAB Field* pogodna za forenziku mobilnih uređaja u terenskim uvjetima te *MSAB Kiosk* i *MSAB Tablet*.

2.2.4. Softverski orijentirani alati za forenziku mobilnih uređaja

Tvrtka *Cellebrite* osim hardverskih alata također proizvodi i softverske alate za forenziku mobilnih uređaja. Proizvode niz proizvoda za prikupljanje i pregled podataka, analizu i istragu te upravljanje i zaštitu. Neki od poznatijih softverskih alata navedene tvrtke su: *Cellebrite Physical Analyzer*, *Cellebrite Premium*, *Cellebrite Reader*, *Cellebrite Frontliner* itd.

Cellebrite Physical Analyzer je softverski alat za forenzičku analizu prikupljenih podataka koji pomaže pri pronalasku ključnih digitalnih dokaza, praćenju događaja te istraživanju digitalnih podataka. Korištenjem određenih inteligentnih mehanizama donosi

odluke gdje treba usmjeriti istraživanje digitalnih podataka. Softver može kreirati priču prema vremenskom slijedu pronađenih digitalnih dokaza. Ima mogućnost dekodiranja podataka u čitljiv oblik te mogućnost unosa podataka različitih formata kao što su podaci prikupljeni *Cellebrite UFED*-om, *Cellebrite Premium* itd. Vrlo važna mogućnost ovog softverskog alata je jednostavno kreiranje izvještaja prema odabranim ključnim podacima.

Cellebrite Reader je softverski alat koji omogućava jednostavan pregled prikupljenih digitalnih dokaza te isticanje važnih podataka. Pruža mogućnost naprednog pretraživanja, filtriranja, pregled pomoću vremenske trake, pronalazak ključnih detalja i slično. Alat se jednostavno upotrebljava bez potrebe za instalacijom, [9].

Osim navedenih *Cellebrite* softverskih alata, na tržištu su također popularni alati poput MSAB, *Autopsy*, *Kali Linux, Oxygen Forensics, ExifTool* i slični drugi alati. MSAB pruža softverske alate na različitim hardverskim platformama kao što je već navedeno u prethodnom potpoglavlju. XRY proizvodi tvrtke MSAB upotrebljavaju se za razne vrste ekstrakcije podataka s mobilnih uređaja, kao što su logička ekstrakcija, fizička ekstrakcija, *Cloud* ekstrakcija i ostali oblici ekstrakcije. Također, MSAB nudi proizvode poput XRY kamere koja omogućava snimanje digitalnih dokaza s mobilnog uređaja HD kvalitetom. *XRY PinPoint* omogućava ekstrakciju i dekodiranje podataka s nestandardnih mobilnih uređaja, kao što su jeftine imitacije određenih proizvođača. Osim proizvoda za ekstrakciju, MSAB također nudi i proizvode za analizu ekstrahiranih podataka. To su proizvodi sa oznakom XAMN, poput *XAMN Viewer, XAMN Spotlight, XAMN Elements* te *XAMN Horizon,* [10].

Autopsy alat može se koristiti za analizu podataka s mobilnih uređaja koji imaju Android i iOS operativne sustave. Alat sadrži određene module poput *Android Analyzer Modula* koji omogućava analizu SQLite te drugih datoteka na Android uređajima. Navedeni modul ima mogućnost ekstrakcije tekstualnih poruka, kontakata, logova poziva, GPS podataka s web preglednika i *Google Maps* aplikacije te slične druge podatke. Također, alat sadrži dodatno i druge module vezane za ekstrakciju podataka sa mobilnih uređaja.

Oxygen Forensics proizvodi više vrsta softverskih alata koji su namijenjeni za ekstrakciju podataka s mobilnih uređaja, dekodiranje i analizu ekstrahiranih podataka. *Oxygen Forensic Detective* softverski je proizvod koji pruža sve usluge u jednom alatu. Omogućava

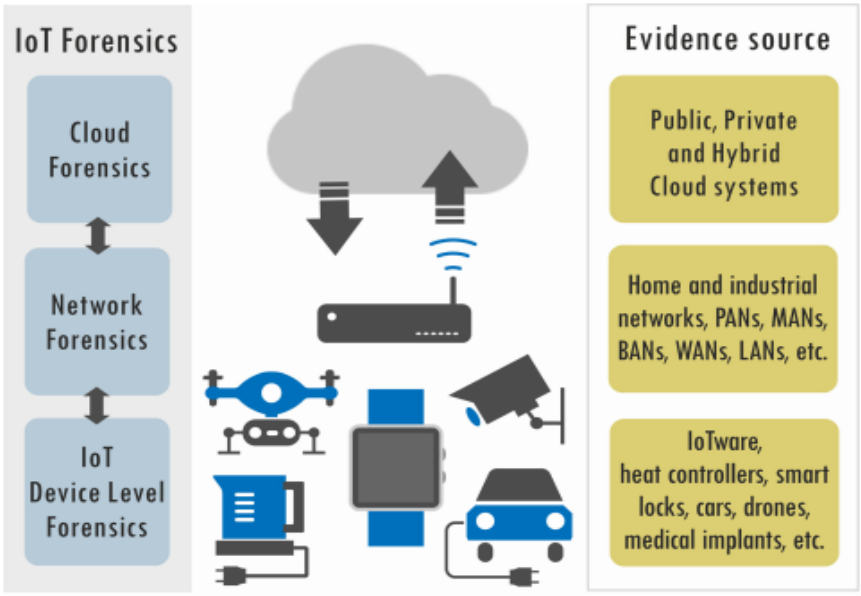
ekstrakciju, dekodiranje i analizu podataka. *Oxygen Forensic Extractor* softversko je rješenje koje omogućava ekstrakciju podataka s mobilnih uređaja na Android i iOS operativnim sustavima. Također, postoji alat *Oxygen Forensic Viewer* koji omogućava istražiteljima dijeljenje ekstrahiranih podataka i analiziranih digitalnih dokaza. Navedene podatke koji su ujedno i dokazi, moguće je dijeliti s drugim istražiteljima ili autoriziranim osobljem kojima je potreban uvid u navedene podatke vezane za forenzičku istragu, [11].

2.3. Ostali oblici digitalne forenzike

Ostali oblici digitalne forenzike podrazumijevaju *Cloud* forenziku, forenziku baza podataka, IoT forenziku, forenziku podataka, forenziku dokumenata, web forenziku, forenziku društvenih mreža te svaki drugi oblik forenzike koji obuhvaća forenzičku istragu nad određenim hardverom ili softverom digitalnog uređaja. U nastavku potpoglavlja ukratko će se opisati *Cloud* forenzika i IoT forenzika.

Cloud forenzika ili forenzika sustava računalstva u oblaku je primjena znanstvenih načela, tehnološke prakse te dokazanih metoda kako bi se rekonstruirali događaji iz prošlosti unutar sustava računalstva u oblaku. Sastoji se od faza identifikacije, prikupljanja dokaza, očuvanja dokaza, ispitivanja i tumačenja dokaza, izvještavanja o potencijalnim digitalnim dokazima te donesenih zaključaka. Osim postojećih izazova koji su prisutni i kod drugih oblika digitalne forenzike, *cloud* forenzika specifična je zbog virtualizacije, velike količine obrađenih podataka te kontinuiranog rasta broja mobilnih i drugih uređaja koji koriste sustave računalstva u oblaku, [12].

Internet of Things (IoT) forenzika relativno je novo i neistraženo područje digitalne forenzike. Može obuhvaćati ostale oblike digitalne forenzike, kao što su mrežna forenzika te *Cloud* forenzika. Na slici 5 prikazane su komponente IoT forenzike.



Slika 5. Komponente IoT forenzike, [13]

Slika 5 prikazuje 3 razine IoT forenzike: *Cloud* forenziku, mrežnu forenziku i forenziku IoT uređaja. *Cloud* forenzika podrazumijeva javne, privatne i hibridne sustave računalstva u oblaku. Mrežna forenzika obuhvaća sve kućne i industrijske mreže, dok forenzika IoT uređaja obuhvaća sve vrste senzora, sustava za nadzor, medicinske implantate, automobile, dronove, pametne brave itd, [13].

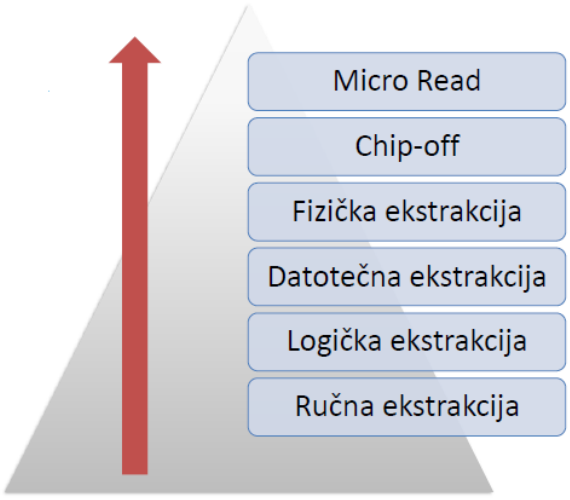
Svakim danom sve veći broj uređaja pristupa internetskoj mreži te se sve više razvija *machine-to-machine* (M2M) komunikacija koja je temelj IoT. Samim time, otvara se prostor za kibernetičke napade kojima počinitelji pokušavaju pristupiti određenim dijelovima mreže ili pametnim kućama, vozilima te drugim komponentama IoT sustava kako bi nanijeli određenu štetu ili ukrali podatke. Neovlaštenim pristupom u mrežu ili sustav, postaje dostupan vrlo veliki broj informacija i podataka te se može nanijeti velika šteta. Iz tog razloga, vrlo je važno takve sustave zaštititi od kibernetičkih napada te nastaviti razvijati razne metode IoT forenzike.

3. EKSTRAKCIJA PODATAKA MOBILNIH UREĐAJA

Ekstrakcija podataka mobilnih uređaja predstavlja postupak izvlačenja podataka, kako bi se mogla provesti forenzička analiza nad ekstrahiranim podacima. Postoje razne vrste ekstrakcije podataka mobilnih uređaja, a to su, [2]:

- ručna
- logička
- datotečna
- fizička
- ostale metode.

Na slici 6 prikazane su metode ekstrakcije podataka sa mobilnih uređaja prema složenosti provedbe te količini ekstrahiranih podataka.



Slika 6. Metode ekstrakcije podataka, [2]

U smjeru strelice, odnosno prema vrhu piramide povećava se složenost provođenja ekstrakcije podataka, dulje vrijeme analize te je potrebno više stručnog znanja za provedbu. Metode ekstrakcije podataka sa slike 6 detaljnije će se prikazati u sljedećim potpoglavljima.

3.1. Ručna ekstrakcija

Ručna metoda ekstrakcije podataka s mobilnih uređaja uključuje ručno traženje podataka na uređaju koji je predmet forenzičke istrage. Ova metoda podrazumijeva korištenje tipkovnice i zaslona na dodir koji se nalaze na mobilnom uređaju koji istražujemo. Digitalni dokazi se prilikom ovakvog oblika ekstrakcije dokumentiraju fotografiranjem. Prednost ručne ekstrakcije je jednostavnost i brzina ekstrakcije, dok su glavni nedostaci količina ekstrahiranih podataka, mogućnost ljudske pogreške te moguće neuočavanje određenih ključnih digitalnih dokaza. Ručna ekstrakcija ne omogućuje povratak izbrisanih podataka, [14].

Također, prilikom ručnog prikupljanja podataka uvijek postoji rizik od slučajnog brisanja podataka koji su mogući digitalni dokazi. Osim navedenog, u slučaju oštećenja mobilnog uređaja, slučaju zaključanog uređaja ili sličnih situacija nije moguće provesti ručnu ekstrakciju. Ručnom ekstrakcijom moguće je prikupiti podatke poput kontakata, povijesti poziva, SMS i MMS poruka, e-mail poruka, povijesti web preglednika, video zapise, fotografije, dokumente, podatke sa društvenih mreža i slično. Postoje određeni alati poput *Project-A-Phone* koji omogućavaju snimanje fotografija i video zapisa cijelog procesa prikupljanja podataka. Prikupljeni podaci mogu biti vidljivi odmah na računalu koje je povezano s alatom. Na slici 7 prikazan je hardverski alat *Cellebrite UFED* kamera, koja omogućava ručno ekstrahiranje podataka.

Slika 7. Cellebrite UFED kamera, [15]

Pomoću *Cellebrite UFED* kamere provodi se ručna ekstrakcija podataka na način da se snima zaslon mobilnog uređaja. Digitalni dokazi prikupljaju se snimanjem fotografija, video zapisa podataka, odnosno direktnim snimkama zaslona.

3.2. Logička ekstrakcija

Logička ekstrakcija zahtijeva povezivanje mobilnog uređaja s forenzičkim alatom za ekstrakciju podataka. Povezivanje se može izvršiti na više načina, odnosno moguće je povezati mobilni uređaj putem USB kabela, RJ-45 kabela, pomoću Bluetootha te na razne ostale načine. Nakon povezivanja računalo inicira naredbu prema mobilnom uređaju. Naredba se interpretira od strane procesora mobilnog uređaja te se zatim traženi podaci šalju prema forenzičkoj radnoj stanici. Generalno gledajući, izbrisani podaci nisu dostupni logičkom ekstrakcijom. Također, logička ekstrakcija zahtijeva određeno poznavanje alata s kojim se radi. Potreban je određeni broj kabela za povezivanje uređaja i alata za forenziku te nije moguće zaobići zaključan ili zaštićen uređaj. Moguće je izvlačenje podataka logičkom ekstrakcijom i bez *root* pristupa, no *root* pristup omogućiti će prikupljanje znatno većeg broja podataka, [14].

Kao prednosti logičke ekstrakcije podataka mogu se navesti jednostavnost, brzina te ekstrakcija veće količine podataka u odnosu na ručnu ekstrakciju. Primjer alata za ovakav oblik ekstrakcije su *MSAB XRY Logical* te *UFED Logical Analyzer* koji se primjenjuje za analizu podataka. Također se i distribucija Santoku Linux može koristiti za logičku ekstrakciju podataka.

Logička ekstrakcija može se provoditi sa prethodno navedenim alatima, a isto tako može se provesti pomoću *adb pull* naredbi te pomoću davatelja sadržaja. Korištenjem *adb* naredbenog retka mogu se izvući svi podaci sa uređaja ili prikupiti samo relevantni te točno traženi podaci. Za pristup uređaju preko *adb* potrebno je osigurati otključan uređaj te omogućenu opciju USB ispravljanje pogrešaka, odnosno *USB debugging* opciju. Podaci aplikacija mogu biti spremljeni na razne lokacije, kao što su: interna pohrana, eksterna pohrana, datoteke zajedničkih postavki te u SQLite baze podataka. Povlačenje podataka sa tih lokacija provodi se upravo pomoću *adb pull* naredbi te se na taj način povlače podaci sa

eksterne pohrane na Desktop ili drugu definiranu lokaciju na uređaju. Korištenjem *SQLite Database Browsera* olakšava se analiza ekstrahiranih podataka iz baza podataka. Razlog tome je tablični prikaz ekstrahiranih podataka. Također, jedan od korisnih alata za analizu podataka prikupljenih iz baza podataka je alat *Oxygen Forensic SQLite Database Viewer*.

Mehanizam korištenja davatelja sadržaja omogućava dijeljenje podataka s drugim aplikacijama, što je većinom način na koji komercijalni forenzički alati funkcioniraju. Moguće je kreirati aplikaciju koja dohvaća sve informacije od svih dostupnih davatelja sadržaja. Prednost ovakve metode logičke ekstrakcije je što se može koristiti na uređajima sa i bez *root* pristupa. Primjer za ovakav oblik logičke ekstrakcije je alat *AFLogical* koji omogućava pristup informacijama kroz navedeni mehanizam te ekstrahirane podatke pohranjuje na SD karticu u CSV formatu. Također, i u ovom slučaju je potrebno imati otključan uređaj te omogućenu *USB Debugging* opciju.

3.3. Datotečna ekstrakcija

Datotečna ekstrakcija podrazumijeva dio logičke ekstrakcije koji je prema složenosti provedbe i količini podataka između općenite logičke ekstrakcije te fizičke ekstrakcije podataka. Pomoću datotečne ekstrakcije mogu se prikupiti svi podaci koji se nalaze u dijelu memorije koji se smatra zauzetim, tj. u alociranom dijelu memorije uređaja. Datotečnom ekstrakcijom može se doći do određenih obrisanih podataka, privremenog sadržaja te podataka koji su ostaci prijašnjih datoteka pohranjenih na istom prostoru. Podaci koji se mogu prikupiti datotečnom ekstrakcijom su: log zapisi, podaci o sustavu, povijest pretraživanja, baze podataka instaliranih aplikacija, povijest korištenja aplikacija, struktura podataka i slično, [2].

Jedna od metoda koju možemo smatrati oblikom datotečne ekstrakcije je već spomenuta *Android Debug Bridge (adb)* metoda. Pomoću *adb* naredbenog retka može se ostvariti komunikacija te kontrola mobilnog uređaja koji je predmet forenzičke istrage. Kao što je već spomenuto ranije u tekstu, prilikom korištenja *adb* metode potrebno je omogućiti *USB Debugging* opciju koja omogućava komunikaciju između mobilnog uređaja te radne

stanice na kojoj je instaliran Android SDK. Mobilni uređaj i radnu stanicu potrebno je povezati odgovarajućim USB kabelom, [16].

Za provedbu datotečne ekstrakcije podataka potrebno je imati otključan uređaj. Zaključavanje zaslona mobilnog uređaja moguće je provesti raznim mehanizmima poput zaključavanja izgledom lica, glasom, PIN-om, uzorkom, alfanumeričkom lozinkom i sličnim drugim mehanizmima. Postoje razne tehnike zaobilaženja zaključanog zaslona mobilnog uređaja, a jedna od njih je pomoću *adb* metode. Navedena metoda izvodi se povezivanjem uređaja s radnom stanicom te unosom sljedeće naredbe: *adb.exe shellcd /data/systemrm gesture.key.* Naredbom se briše datoteka *gesture.key* te se nakon toga provodi ponovno podizanje sustava (*reboot*) i unosi se nasumice odabran uzorak ukoliko se ponovno zatraži unos uzorka za otključavanje. Drugi način je spajanjem mobilnog uređaja s forenzičkom radnom stanicom putem USB kabela te unosom naredbe:

adb.exe
shellcd /data/data/com.android.providers.settings/databasessqlite settings.dbsqlite>update system set value=0 where name='lock_pattern_autolock';sqlite>update system set value=0 where name= 'lockscreen.lockedoutpermenantly';

Nakon unosa naredbe uređaj se ponovno pokrene i time je završeno ažuriranje *settings.db* datoteke. Ukoliko uređaj i dalje nije otključan, potrebno je obrisati *gesture.key* datoteku kao što je već opisano gore u tekstu.

Sljedeći način na koji je moguće otključati uređaj je tzv. „*smudge attack*“. To je jednostavna metoda na kojoj se može prepoznati uzorak za zaključavanje zaslona pomoću mrlja na zaslonu mobilnog uređaja. Praktično je vrlo mala vjerojatnost da će se pomoću ove metode otkriti uzorak zaključavanja zaslona mobilnog uređaja. Razlog tome je što korištenje mobilnog uređaja ostavlja mrlje na zaslonu na dodir te je vrlo teško otkriti uzorak kojim je mobilni uređaj zaključan. Na slici 8 prikazana je „*smudge attack*“ metoda.

Slika 8. „*Smudge* attack*“* metoda, [17]

Uz poznato korisničko ime i lozinku primarnog Gmail računa konfiguriranog na mobilnom uređaju također je moguće promijeniti lozinku za zaključavanje uređaja. Nakon određenog broja neuspješnih pokušaja otključavanja zaslona, pojavljuje se opcija „Zaboravljena zaporka“ uz pomoć koje se može postaviti nova zaporka. Na većini novih mobilnih uređaja postavljena je opcija kojom se treba izbrisati sve podatke s uređaja prilikom postavljanja nove zaporke za zaključavanje zaslona.

3.4. Fizička ekstrakcija

Fizička ekstrakcija podrazumijeva tzv. „*bit-by-bit*“ kopiranje podataka s fizičke pohrane. Kao rezultat takvog kopiranja dobije se slika memorije u binarnom formatu. Informacije i podaci se prikupljaju direktnim pristupom *flash* memoriji koja je nepromjenjiva te se primarno koristi kod memorijskih kartica i USB *flash* diskova kao SSD memorija. Fizičkom ekstrakcijom kopira se cijeli datotečni sustav uređaja bit po bit, uključujući izbrisane datoteke te nedodijeljeni prostor memorije uređaja. Prikupljeni podaci zahtijevaju visoku razinu stručnog znanja za analizu te je sami postupak ekstrakcije podataka složeniji od prethodno navedenih. Sadržaj koji se može prikupiti ovakvim oblikom ekstrakcije uključuje sav logički sadržaj dostupan korištenjem aplikacijskog programskog sučelja (*Application Programming Interface – API*). Također, može se prikupiti obrisan i skriven sadržaj te sadržaj

koji mobilni uređaj prikuplja bez interakcije s korisnikom, a ponekad i bez znanja korisnika kao što su GPS lokacije, lista Wi-Fi mreža, korištenje sesije web preglednika, razni podaci sustava i slično, [2] i [14].

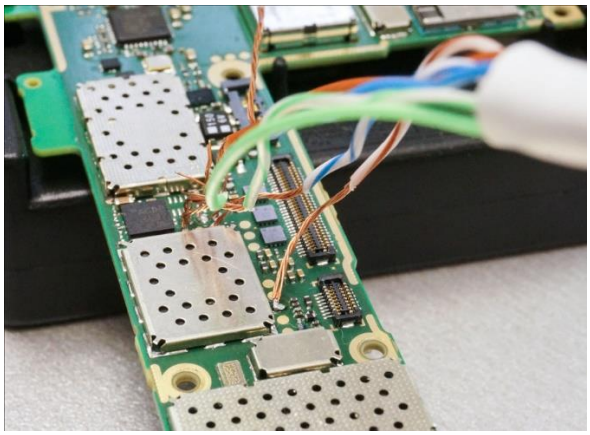
Najznačajnija prednost ovakvog oblika ekstrakcije podataka je količina ekstrahiranih podataka te mogućnost ekstrahiranja izbrisanih podataka, a zatim i mogućnost zaobilaženja zaporke zaključavanja zaslona mobilnog uređaja. Glavni nedostaci ovakvog oblika ekstrakcije su teža interpretacija i dekodiranje podataka, zatim dulje vrijeme potrebno za ekstrakciju i analizu prikupljenih podataka. Također, kao nedostatak može se smatrati potrebna veća stručnost i veće znanje za provedbu fizičke ekstrakcije u odnosu na ostale oblike ekstrakcije podataka.

3.4.1. Invazivne metode fizičke ekstrakcije

Invazivne metode fizičke ekstrakcije su one metode koje zahtijevaju fizičko rastavljanje mobilnog uređaja kako bi se provela ekstrakcija podataka. Neke od invazivnih metoda fizičke ekstrakcije su: *JTAG, Chip off, ISP – eMMC, Micro Read* itd.

Joint Test Action Group (JTAG) je napredna invazivna metoda fizičke ekstrakcije koja koristi testne priključne portove (*test access ports – TAP*) kako bi se mogao ostvariti pristup neobrađenim podacima pohranjenim na mobilnim uređajima. Ovaj proces uključuje korištenje postojećih točki lemljenja na elektronskoj pločici. JTAG ekstrakcija podataka zahtijeva odgovarajuću opremu i odgovarajući JTAG kabel kako bi se mogla provesti ekstrakcija svih podataka sa mobilnog uređaja. Metoda se može provoditi na uređajima s Android i iOS operativnim sustavima, a isto tako i na Windows Phone uređajima. Prednosti navedene metode su: velika količina ekstrahiranih podataka, mogućnost ekstrahiranja izbrisanih podataka te mogućnost prikupljanja podataka s zaključanih, oštećenih i na drugi način nepristupačnih mobilnih uređaja. Prilikom provođenja ove invazivne metode ekstrakcije, potrebni su stručnjaci s velikim znanjem te se sam proces ekstrakcije provodi uz veliki oprez. Uz pažljivo i oprezno provođenje, mobilni uređaj bit će operabilan i nakon provedene ekstrakcije podataka. Prije bilo kojeg oblika invazivne fizičke ekstrakcije podataka, uvijek je

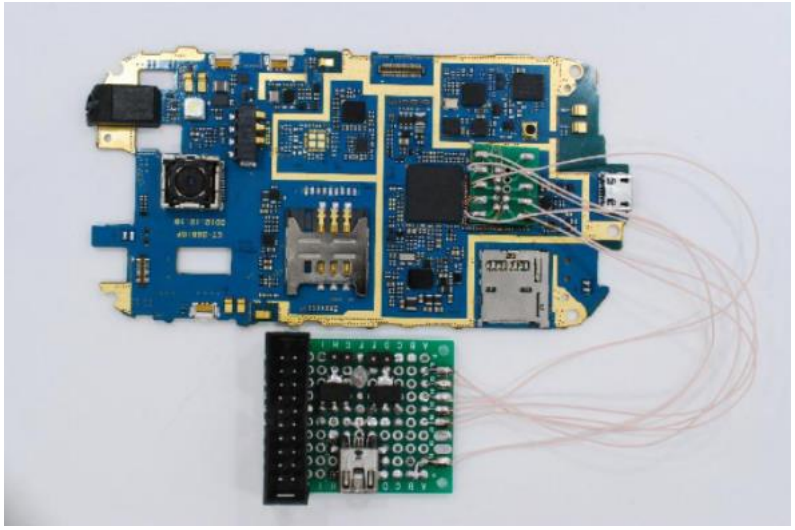
potrebno pokušati ekstrahirati podatke s komercijalnim forenzičkim alatima koji ne stvaraju rizik od oštećenja mobilnog uređaja. No, u slučaju da nije moguće zaobići zaštitu mobilnog uređaja te omogućiti *USB debugging* opciju, tada je potrebno pristupiti ovakvom obliku invazivne fizičke ekstrakcije podataka. Ukoliko je omogućena enkripcija cijelog diska mobilnog uređaja, JTAG će napraviti ekstrakciju neobrađene (*raw*) slike uređaja te probijanje enkripcije može biti jedna od opcija, [18]. Na slici 9 prikazana je JTAG metoda ekstrakcije podataka mobilnog uređaja.



Slika 9. JTAG metoda ekstrakcije, [18]

Sljedeća invazivna fizička metoda ekstrakcije podataka je *Chip-off* metoda. *Chip-off* metoda je destruktivna metoda zbog toga što zahtijeva uklanjanje, odnosno odlemljivanje čipa *flash* memorije uređaja ili priključivanje žica na PCB kontakte. Prema količini ekstrahiranih podataka ova metoda približno je jednaka prethodno opisanoj JTAG metodi. Prilikom provođenja forenzičke istrage te ekstrakcije *chip-off* metodom, istražitelji se mogu suočiti s kriptiranom particijom gdje ne mogu pronaći dekripcijske ključeve. Također, Apple uređaji, mnogi Samsung uređaji i poneki ostali uređaji imaju prisilnu „*out-of-the-box*“ enkripciju koja se ne može zaobići prilikom *chip-off* ekstrakcija čak i ako je ispravna lozinka poznata. Ukoliko je na mobilnom uređaju cijeli disk kriptiran, ovom metodom dobiti će se kriptirana slika diska za koju postoji određena vjerojatnost da će se uspješno dekriptirati. Na Android verzijama poslije verzije 5.0 kriptiraju se metapodaci sa glavnim ključem, tzv. „*master key*“, koji je pohranjen u zaštićenom području kojem se ne može pristupiti putem *chip-off* metode. Upravo zbog toga navedena metoda koristi se u većini slučajeva tek nakon provedene određene druge neinvazivne fizičke metode ekstrakcije i JTAG metode, [18].

In-System Programming (ISP) je nedestruktivna varijacija *chip-off* metode ekstrakcije podataka pomoću koje forenzički istražitelji mogu doći do podataka na eMMC memoriji bez uklanjanja čipa. Navedenu metodu moguće je koristiti isključivo na uređajima koji sadrže eMMC čipove, a to su *flash* čipovi koji integriraju *flash* memoriju i kontroler u jedan modul. Na slici 10 prikazana je ISP metoda gdje je eMMC adapter povezan sa PCB kontaktima mobilnog uređaja.



Slika 10. eMMC adapter povezan sa PCB kontaktima mobilnog uređaja, [18]

Micro read je proces koji uključuje ručno gledanje i interpretiranje podataka prikupljenih na memorijskom čipu. Prilikom provođenja ove metode forenzički istražitelji koriste elektronski mikroskop pomoću kojeg analiziraju fizičke ulaze na čip te prevode status na pojedinim ulazima u 0 ili 1 kako bi detektirali odgovarajuće ASCII znakove. *Micro read* metoda je skupa, zahtijeva visoko znanje i stručnost te dosta vremena potrebnog za analizu podataka. Većinom se primjenjuje isključivo u najvažnijim slučajevima koji ugrožavaju nacionalnu sigurnost te tek nakon iscrpljenih svih ostalih tehnika i metoda ekstrakcije podataka, [14].

3.4.2. Neinvazivne metode fizičke ekstrakcije

Neinvazivne metode fizičke ekstrakcije podataka su one koje ne zahtijevaju rastavljanje mobilnog uređaja prilikom ekstrakcije podataka. Neke od neinvazivnih metoda

fizičke ekstrakcije podataka su *Android Debug Bridge* (ADB), *Bootloader, Forensic Recovery Partition* itd.

Također, neinvazivnom fizičkom ekstrakcijom podataka može se smatrati i korištenje softverskih alata poput *Cellebrite Physical Analyzer* i *MSAB XRY Physical*. Takvi softverski alati omogućuju ekstrakciju raznih aplikacijskih podataka na mobilnim uređajima, povratak izbrisanih datoteka, napredno dekodiranje podataka, omogućavaju pristup sustavu uređaja i zaštićenim podacima, svladavanje zaključanih i kriptiranih uređaja, HEX analizu podataka, *hash* algoritme itd.

4. SANTOKU LINUX DISTRIBUCIJA ZA FORENZIČKU ANALIZU MOBILNIH UREĐAJA

Santoku Linux distribucija specijalizirana je Linux platforma koja sadrži veliki izbor alata namijenjenih za provedbu forenzičke istrage mobilnih uređaja. Može se koristiti za sljedeća tri područja: mobilnu forenziku, analizu mobilnih zlonamjernih softvera te za testiranje sigurnosti mobilnih uređaja. Santoku Linux distribucija obuhvaća širok izbor alata za prikupljanje podataka s mobilnih uređaja te za njihovu analizu. Osim toga, sadrži emulatore mobilnih uređaja, omogućava simulaciju mrežnih servisa za dinamičku analizu, pristup bazama zlonamjernih softvera te razne druge mogućnosti vezane za analizu takvih oblika softvera. Također, navedena Linux distribucija sadrži skripte koje omogućavaju detekciju zajedničkih problema u mobilnim aplikacijama te razne mogućnosti za testiranje drugih elemenata sigurnosti mobilnih aplikacija, [19].

Santoku Linux dolazi s ugrađenim *Software Development Kit* (SDK) okvirom, hardverskim upravljačkim programima (e. *driverima*) i svim alatima potrebnim za automatsku detekciju uređaja i uparivanje. Navedena Linux distribucija besplatan je i otvoreni projekt koji omogućava korisnicima provođenje forenzike, procjenu i testiranje sigurnosti mobilnih uređaja.

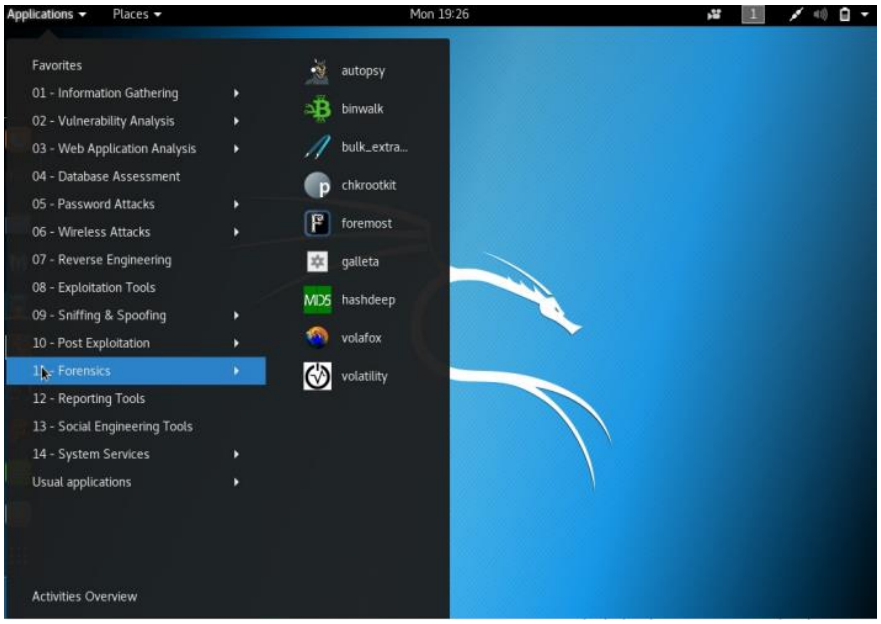
4.1. Linux distribucije za forenziku mobilnih uređaja

Linux sustavi mogu se koristiti u području forenzičke analize mobilnih uređaja, a isto tako i u području penetracijskog testiranja. Većina Linux distribucija za forenzičku analizu mobilnih uređaja dolazi sa besplatnim *open-source* alatima za analizu prikupljenih digitalnih dokaza. Osim Santoku Linux distribucije, za forenziku mobilnih uređaja također se koriste sljedeće distribucije:

- Kali Linux
- DEFT
- Parrot

- Blackbuntu
- Paladin Linux
- CAINE itd.

Kali Linux izgrađen je na Debian platformi, u današnje vrijeme smatra se najpopularnijom Linux distribucijom. Od navedenih distribucija sadrži najveći broj forenzičkih alata, alata za probijanje lozinki, alata za izvještavanje te raznih drugih alata. Sadrži razne aplikacije i alate za prikupljanje informacija, analizu ranjivosti sustava, analizu web aplikacija, napade na zaporke, obrnuti inženjering, forenziku i slično. Pod kategorijom forenzičkih alata sadrži alate poput *Autopsy*, *binwalk*, *bulk_extraction*, *foremost*, *hashdeep*, *volatility* te ostale alate kao što je vidljivo na slici 11. Slika 11 prikazuje korisničko sučelje Kali Linux distribucije, [20].



Slika 11. Prikaz korisničkog sučelja Kali Linuxa, [20]

Digital Evidence and Forensics Toolkit (DEFT) dolazi u dvije verzije, a to su puna verzija i *DEFT Zero* verzija koja ne sadrži alate za forenziku mobilnih uređaja i probijanje zaporki. DEFT distribucija sadrži nekoliko forenzičkih kategorija, a to su: analiza, *anti-malware*, oporavak podataka, *hashing*, slike digitalnih sustava, mrežna forenzika, mobilna forenzika, oporavak podataka i alati za izvješćivanje. Unutar svake navedene kategorije nalazi se određeni broj raznolikih alata dostupnih forenzičkim istražiteljima. Za forenziku mobilnih

uređaja mogu se primijeniti sljedeći alati: *ADB, Fastboot, Bitpim, Apktool, Ipddump, idevicebackup2, iphonebackupanalyzer2*, [21].

Parrot je Linux distribucija bazirana na Debianu koja je uglavnom usredotočena na kibernetičku sigurnost i forenziku. Sadrži detaljno i moderno grafičko korisničko sučelje te predstavlja prvu distribuciju na svijetu koja je predstavila antiforenzičke alate.

Blackbuntu je Linux distribucija koja se većinom upotrebljava za penetracijsko testiranje i digitalnu forenziku, a dizajnirana je također i za računalnu, informacijsku te Internet sigurnost.

Paladin Linux baziran je na Ubuntu te sadrži preko 100 raznih alata podijeljenih u 33 kategorije. Na taj način čini distribuciju pogodnu za izvršenje raznih forenzičkih izazova. Također, unutar Paladin Linuxa dodan je alat *Autopsy* koji predstavlja snažan forenzički alat primjenjiv u značajnom broju forenzičkih istraga. Sadrži alate za analizu logova, mailova, Internet analizu, analizu zlonamjernih softvera itd.

Computer Aide Investigation Environment (CAINE) predstavlja javno dostupnu Linux distribuciju za kompletnu digitalnu forenzičku istragu s jednostavnim grafičkim korisničkim sučeljem. Sadrži razne alate za forenzičku analizu diska, memorije, baza podataka, mobilnu forenziku, mrežnu forenziku i slično. Također, sadrži direktne poveznice na alate kao što su *Guymager* i *Autopsy*.

4.2. Mogućnosti i značajke Santoku Linux distribucije

Mogućnosti Santoku Linux distribucije za forenziku mobilnih uređaja možemo prikazati kroz tri različita područja. Područja primjene Santoku Linuxa možemo podijeliti na: mobilnu forenziku, zlonamjerne softvere te sigurnost mobilnih uređaja. Unutar područja mobilne forenzike mogu se svrstati alati navedene distribucije koji se primjenjuju za prikupljanje i analizu prikupljenih podataka. To su alati koji služe za prikupljanje podataka iz memorije mobilnih uređaja. Moguće je prikupljanje podataka iz interne memorije, RAM memorije te raznih oblika eksterne memorije poput raznih memorijskih kartica i slično. Osim toga, unutar Santoku Linux distribucije sadržani su alati za forenzičku analizu prikupljenih

podataka kojima se mogu filtrirati pronađeni podaci. Drugo područje djelovanja Santoku Linux distribucije obuhvaća alate za ispitivanje mobilnih zlonamjernih softvera. Također, unutar ove distribucije postoje određeni emulatori mobilnih uređaja koji mogu biti jako korisni prilikom provođenja forenzičke analize. Emulator se može definirati kao aplikacija koja omogućava prikaz odabranog uređaja i ponašanje uređaja nakon instaliranja određenih aplikacija. Može se omogućiti simulacija mrežnih usluga kako bi se mogla provesti dinamička analiza te je omogućen pristup do baze podataka zlonamjernih softvera. Treće područje djelovanja Santoku Linuxa je područje sigurnosti mobilnih uređaja. Navedeno područje obuhvaća procjenu mobilnih aplikacija vezano za sigurnost te njihov utjecaj na rad mobilnog uređaja. Određenim skriptama mogu se pronaći zajednički problemi unutar aplikacija, dekriptirati binarne datoteke i slično, [19].

4.2.1. Prikupljanje i analiza podataka

Prikupljanje podataka podrazumijeva ekstrahiranje što većeg broja podataka iz mobilnog uređaja, kako bi se došlo do ključnih informacija i digitalnih dokaza koji su značajni za proces forenzičke istrage. Podaci se mogu prikupiti logičkom ekstrakcijom, odnosno korištenjem alata poput *Android Forensics Logical Open Source Edition* (AFLogical OSE). Logičkom ekstrakcijom podataka dohvaćaju se podaci o mobilnom uređaju, kontakti, logovi poziva, SMS i MMS poruke, medijski podaci, podaci aplikacija i slično.

Alati poput *libimobiledevice* i *iOS Backup Analyzer 2* omogućavaju izradu logičke sigurnosne pohrane podataka te njenu analizu na uređajima koji imaju iOS operativni sustav. Proces analize podataka važan je zbog toga što se analizom mogu otkriti određeni ključni dokazi koji na prvi pogled možda nisu uočljivi. Više o samim funkcionalnostima alata Santoku Linux distribucije bit će opisano u sljedećem poglavlju.

4.2.2. Alati za ispitivanje mobilnih zlonamjernih softvera

Ispitivanje mobilnih aplikacija te njihovog utjecaja na rad uređaja moguće je provoditi pomoću emulatora unutar Santoku Linux distribucije. Instaliranje i pokretanje emulatora provodi se pomoću razvojnog alata *Android SDK Manager*. Također, Santoku Linux sadrži određene alate kojima je moguće provesti ispitivanje mobilnih zlonamjernih softvera te detektirati sumnjive aplikacije koje mogu negativno utjecati na rad uređaja.

Alat *APKTool* jedan je od alata koji omogućava detaljnu analizu aplikacija, otklanjanje pogrešaka, dekodiranje resursa u približno izvorni oblik te još mnoge druge značajke kao dio obrnutog inženjeringa. Također, alatima poput *Androguarda, Drozera* i ostalih iz kategorije alata za obrnuti inženjering provodi se ispitivanje aplikacija kako bi se utvrdili određeni nedostaci ili zlonamjerni softver koji može štetno utjecati na rad uređaja ili sustava.

4.2.3. Procjena sigurnosti mobilnih uređaja

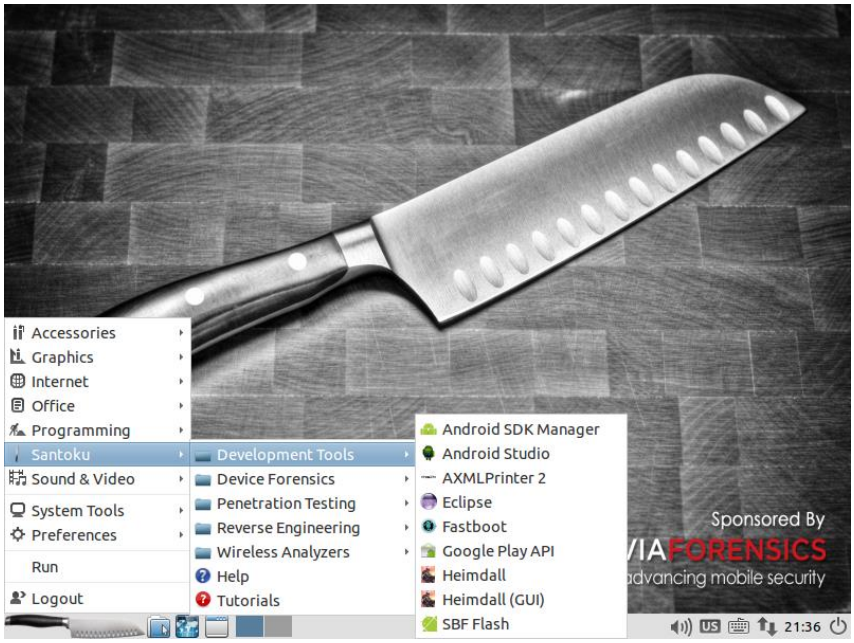
Alatima za penetracijsko testiranje provjerava se i procjenjuje sigurnost mobilnih uređaja kako bi se uočili nedostaci te došlo do procjene stvarnog stanja sigurnosti mobilnog uređaja i korisničkih podataka na njemu. Glavni ciljevi penetracijskog testiranja su identifikacija, popravak i prevencija sigurnosti te uočavanje i uklanjanje svih nedostataka na softverskim aplikacijama. Analiza prometa može se provoditi na dva načina: pasivni i aktivni način. Pasivni način podrazumijeva da osoba koja provodi analizu prometa nema aktivnu interakciju sa aplikacijama u realnom vremenu, već dohvaća mrežne pakete pomoću određenih alata poput *Wiresharka*. Zatim se podaci analiziraju kako bi se uočio određeni nedostatak ili ranjivost. Aktivni način analize prometa podrazumijeva da osoba koja provodi testiranje ima aktivnu interakciju sa aplikacijama koje testira. Također, treba imati postavljen *proxy* na način da ima puni pristup svim zahtjevima odrađenim unutar tog određenog promatranog posredničkog poslužitelja (e. *proxy server*), [22].

Softverskim alatima kao što je *Drozer* moguće je pronaći sigurnosne ranjivosti unutar aplikacija i mobilnih uređaja te detektirati površinu napada ciljane aplikacije. Na taj način dobije se veliki broj detalja, poput eksportiranih aktivnosti aplikacije, davatelja sadržaja te eksportiranih usluga aplikacije. Pomoću *APKTool* alata moguće je provesti tzv. „prepakirani

napad“ kojim se simulira način na koji napadač može hakirati aplikacije. Napadač izmjenjuje APK datoteku na način da ubacuje malicioznu datoteku ili izmjenjuje određene linije koda te zatim obnavlja APK datoteku. Zatim ju potpisuje i objavljuje u javnosti. Žrtve ovakvog oblika napada u većini slučajeva ne mogu prepoznati napad jer su originalna i modificirana APK datoteka gotovo identične. Osim navedenih, postoje još i drugi alati unutar Santoku Linux distribucije koji omogućavaju provedbu penetracijskog testiranja mobilnih uređaja, [22].

5. FUNKCIONALNOSTI ALATA SANTOKU LINUX DISTRIBUCIJE

Alate Santoku Linux distribucije prema funkcionalnostima možemo podijeliti u sljedeće kategorije: razvojni alati, alati za forenziku uređaja, alati za penetracijsko testiranje, alati za obrnuti inženjering te alati za analizu bežičnih mreža. Na slici 12 prikazan je izbornik unutar kojeg su vidljivi alati prema prethodno navedenim kategorijama.



Slika 12. Izbornik alata unutar Santoku Linux distribucije

Unutar svake kategorije nalazi se određeni broj različitih alata koji se koriste ovisno o tome što je forenzičkom istražitelju potrebno te ovisno o tome koji uređaj je predmet forenzičke istrage.

5.1. Razvojni alati

Razvojni alati koriste se od strane razvojnih programera i služe za stvaranje, održavanje, otklanjanje pogrešaka te druge načine podrške programima ili aplikacijama. Pod kategorijom razvojnih alata Santoku Linux distribucije nalaze se sljedeći alati:

- *Android SDK Manager*

- *Android Studio*
- *AXMLPrinter 2*
- *Eclipse*
- *Fastboot*
- *Google Play API*
- *Heimdall/Heimdall(GUI)*
- *SBF Flash.*

Android SDK Manager je alat s naredbenim retkom koji omogućava pregled, instalaciju, deinstalaciju i ažuriranje paketa za Android SDK, [23].

Android Studio je alat koji služi za razvoj Android aplikacija te omogućava razne značajke poput jedinstvenog okruženja za razvoj aplikacija. Sadrži brzi emulator s raznim značajkama. Također, sadrži mogućnost izmjene koda ili dijela izvora pokrenute aplikacije bez potrebe za ponovnim pokretanjem i razne druge značajke.

AXMLPrinter2 alat služi za analizu APK datoteka pomoću kojeg se dobije naziv paketa, broj verzije te ikona u APK datoteci. Jedan je od potrebnih alata za APK dekompilaciju i modifikaciju. Primjerice, može se koristiti ukoliko je potrebno provjeriti dozvole te nazive APK instalacijskog paketa.

Eclipse platforma može se koristiti za razvoj klijentskih aplikacija, integriranih razvojnih okruženja te drugih alata. Navedena platforma razvijena je pomoću Jave te se može koristiti za razvoj alata za računalno programiranje, programe za otklanjanje pogrešaka te alate za testiranje, [24].

Fastboot dijagnostički je alat koji omogućava pristup svim particijama uređaja, uključujući Android sustav na mobilnim uređajima, podatkovne particije, *boot* particije itd. Koristi se za ažuriranje *flash* sustava datoteka na Android uređajima.

Google Play API je usluga koja omogućava zadatke vezane za upravljanje aplikacijama i objavljivanje aplikacija. Omogućava ažuriranje i izdavanje novih verzija aplikacija te uređivanje lista aplikacija na *Google Play Trgovini*. Također, omogućava

upravljanje katalozima proizvoda unutar aplikacija, statusom kupovine proizvoda te pretplatama na aplikacije.

Heimdall alat dostupan je za MAC, Windows i Linux platforme te se koristi za *flashanje firmwarea*, odnosno *read-only* memorije (ROM) na Samsung mobilnim uređajima. Santoku Linux distribucija sadrži *Heimdall* alat s grafičkim korisničkim sučeljem te bez grafičkog korisničkog sučelja.

SBF Flash alat koristi se za SBF datoteke koje predstavljaju datoteke sustava korištene većinom na Android mobilnim uređajima. SBF datoteke se sastoje od sigurnosnih kopija datoteka spremljenih na Android uređaju.

5.2. Alati za forenziku uređaja

Unutar Santoku Linux distribucije postoje alati koji se mogu primijeniti za prikupljanje i analizu podataka koji su ekstrahirani sa mobilnih uređaja. To su sljedeći alati:

- *AF Logical OSE*
- *Android Brute Force Encryption*
- *ExifTool*
- *iOS Backup Analyzer 2*
- *libimobiledevice*
- *scalpel*
- *SleuthKit*
- *Yaffey.*

AF Logical OSE je alat koji forenzičkom istražitelju omogućava ekstrakciju logova poziva, ekstrakciju kontakata s mobilnog uređaja te SMS i MMS poruka. Pomoću navedenog alata provodi se logička ekstrakcija podataka s mobilnog uređaja. Unutar Santoku Linux distribucije, navedeni alat koristi se kroz naredbene retke te se ekstrahirani podaci povlače na SD karticu.

Android Brute Force Encryption alat koristi se za probijanje PIN-a kojim je enkriptiran uređaj kako bi se moglo pristupiti podacima uređaja te ih ekstrahirati, [19].

ExifTool predstavlja softverski alat za čitanje, pisanje i manipulaciju slikama, audio, video, PDF te raznim drugim tipovima metapodataka. Može se koristiti na raznim operativnim sustavima poput Windows, Mac OS, Linux i slično. Navedeni alat može pomoći forenzičarima prilikom istraživanja datuma, vremena, mjesta snimanja fotografije, modela kamere kojom je fotografija snimljena te pri pronalasku raznih drugih sličnih metapodataka.

iOS Backup Analyzer 2 alat je proizvod baziran na Java programskom jeziku te se također može upotrebljavati na raznim platformama poput Windows, Mac i Linux operativnih sustava. Ovaj alat većinom se koristi za ekstrakciju i analizu sigurnosnih kopija podataka, ali isto tako može se koristiti i za izradu sigurnosnih kopija, [25].

Libimobiledevice je alat, odnosno softverska biblioteka koja omogućava pristup datotečnom sustavu uređaja te ima sposobnost povrata podataka o internim komponentama, sigurnosno kopiranim i obnovljenim dokumentima. Sadrži mogućnost upravljanja aplikacijama instaliranim na uređaju, moguće je dohvaćanje liste kontakata, unosa u adresar, oznaka i slično, [26]

Scalpel je vrlo koristan softverski alat koji se primjenjuje u digitalnoj forenzici za oporavak izbrisanih podataka. Alat dohvaća izbrisane podatke iz blokova baza podataka koji se nalaze unutar sustava pohrane uređaja te ih odmah oporavlja. Bez obzira na vrstu datotečnog sustava kojim je disk formatiran, ovaj alat koristi baze podataka s raznim zaglavljima i podnožjima kako bi pratio datoteke različitih tipova.

SleuthKit je kolekcija alata sa naredbenim retkom i C bibliotekom koja omogućava analizu slike diska te oporavak podataka. Može se koristiti na Windows i Unix platformama, ima mogućnost prikaza skrivenih i obrisanih datoteka. *SleuthKit* čini osnovu *Autopsy* alata koji sadrži grafičko sučelje bazirano na *SleuthKit* alatu, [27].

Yaffey je alat s grafičkim korisničkim sučeljem koji se koristi za čitanje, uređivanje i kreiranje YAFFS2 slika. Omogućava kreiranje novih YAFFS2 slika, uređivanje postojećih, eksportiranje i importiranje podataka slike, brisanje, uređivanje i slične druge mogućnosti.

5.3. Alati za penetracijsko testiranje

Penetracijsko testiranje je aktivnost kojom se provodi ispitivanje sigurnosnih propusta i ranjivosti određenog sustava, prije nego su iste otkrivene od strane potencijalnih napadača na sustav. Alati za penetracijsko testiranje imaju ulogu otkrivanja sigurnosnih propusta i ranjivosti sustava, [22].

Unutar kategorije alata za penetracijsko testiranje u Santoku Linux distribuciji nalaze se sljedeći alati:

- *Burp Suite*
- *Ettercap*
- *Nmap*
- *SSLStrip*
- *w3af (konzola/GUI)*
- *ZAP*
- *Zenmap.*

Burp Suite jedan je od najpopularnijih alata u području penetracijskog testiranja. Namijenjen je traženju sigurnosnih ranjivosti te ispitivanju sigurnosti web aplikacija na temelju *proxija*.

Ettercap je također jedan od alata mrežne sigurnosti s otvorenim kodom namijenjen za „*man-in-the-middle*“ napade na LAN mreže. Može se koristiti za analizu protokola računalnih mreža i ispitivanje sigurnosti. Navedeni alat sposoban je za presretanje prometa na određenom mrežnom segmentu, hvatanje zaporki te aktivno prisluškivanje određenih protokola.

Nmap je besplatan alat s otvorenim kodom za otkrivanje mreža i ispitivanje sigurnosti. Koristi IP pakete za otkrivanje informacija o dostupnim *hostovima* na mreži, servisima i aplikacijama te verzijama aplikacija koje *hostovi* nude. Također, koristi se za otkrivanje informacija o operativnim sustavima te drugim raznim karakteristikama. Pogodan je za brzo skeniranje velikih računalnih mreža.

SSLStrip je penetracijski alat koji „otima“ promet na HTTP mreži te prati HTTPS poveznice i preusmjeravanja. Zatim ih preslikava u slične HTTP poveznice ili homografski

slične HTTPS poveznice. Za navedeni alat može se reći da HTTPS web stranice pretvara u HTTP stranice.

W3af je alat koji služi za napade i reviziju web aplikacija. Unutar Santoku Linux distribucije ovaj alat može se naći u dvije verzije, tj. s grafičkim korisničkim sučeljem (GUI) te kao konzola. Cilj primjene ovog alata je pronaći i iskoristiti sve ranjivosti web aplikacija kako bi se iste unaprijedile te kako bi se povećala njihova sigurnost.

Zed Attack Proxy (ZAP) je besplatan alat s otvorenim kodom za penetracijsko testiranje web aplikacija. Ovaj alat nalazi se između preglednika ispitivača te web aplikacija. Na taj način može presretati i provjeravati sve poruke između preglednika i web aplikacije. Može modificirati sadržaj a zatim proslijediti te pakete na odredište.

Zenmap je alat otvorenog koda primjenjiv na različitim platformama poput Linuxa, Windowsa, Mac OS, BSD itd. Napravljen je kako bi omogućio jednostavno korištenje *nmapa* korisnicima a isto tako pružio napredne značajke za iskusnije korisnike. Alat pruža mogućnost spremanja rezultata skeniranja u bazu podataka kako bi se isti mogli usporediti sa naknadnim skeniranjima.

5.4. Alati za obrnuti inženjering

Obrnuti inženjering je proces kojim se ispituju detaljne informacije i specifikacije uređaja, procesa, sustava te dijela softvera u svrhu zaštite. Isto tako obrnuti inženjering koristi se kako bi se detektirali i neutralizirali virusi i svi drugi oblici zlonamjernog softvera. Unutar Santoku Linux distribucije nalaze se sljedeći alati iz kategorije alata za obrnuti inženjering:

- *Androguard*
- *AntiLVL*
- *APKTool*
- *Baksmali*
- *Bulb Security SPF*
- *Dex2jar*

- *Drozer*
- *Jasmin*
- *JD-GUI*
- *Procyon*
- *Radare2*
- *Smali.*

Androguard alat zasnovan je na *Phyton* programskom jeziku te se koristi za obrnuti inženjering Android aplikacija.

AntiLVL se primjenjuje za kompromitiranje standardnih metoda zaštite licenci kao što je *Android License Verification Library* (LVL).

APKTool je alat za obrnuti inženjering koji ima mogućnost dekodiranja resursa u gotovo izvorni oblik te ih može obnoviti nakon određenih promjena što omogućava ispravak *Smali* koda korak po korak.

Smali/Baksmali je alat za montažu, odnosno rastavljanje *dex* formata korištenog od strane *dalvik*. *Dalvik* predstavlja diskontinuirani proces virtualnog stroja koji se koristi u Googleovom Android operativnom sustavu.

Dex2jar je alat koji radi s Android *.dex* i Java *.class* datotekama. Omogućava čitanje i pisanje *.dex* datoteke, pretvaranje *.dex* datoteka u *.class* datoteke i slične druge mogućnosti.

Drozer alat omogućava traženje sigurnosnih ranjivosti aplikacija i uređaja. Također, omogućava funkcionalnosti koje pomažu pri korištenju, dijeljenju i razumijevanju javne eksploatacije Android uređaja.

Jasmin je alat za penetracijsko testiranje s otvorenim kodom za JavaScript. Pruža funkcionalnosti koje se mogu koristiti za pokretanje automatiziranih testova sinkronog i asinkronog koda.

JD-GUI je samostalna grafička funkcionalnost koja omogućava prikaz Java izvornog koda *.class* datoteka.

Procyon je paket Java alata za metaprogramiranje usmjeren na generiranje i analizu koda.

Radare2 je alat otvorenog koda koji se primjenjuje za obrnuti inženjering te pruža funkcionalnosti poput statičke i dinamičke analize, digitalne forenzike ili eksploatacije softvera te podržava razne platforme, arhitekture i binarne formate.

5.5. Alati za analizu bežičnih mreža

Bežične mreže primjenjuju se svakodnevno za razne usluge te uključuju povezivanje različitih uređaja poput računala, prijenosnih računala, video igara, mobilnih uređaja, digitalnih kamera, tableta, pametnih televizija i još mnogih drugih uređaja. Alati za analizu bežičnih mreža služe kako bi se detektirale sigurnosne prijetnje te otkrile ranjivosti bežične mreže. Unutar Santoku Linux distribucije nalaze se sljedeći alati za analizu bežičnih mreža:

- *Chaosreader*
- *Dnschef*
- *DSniff*
- *Mitmproxy*
- *Tcpdump*
- *Wifite*
- *Wireshark.*

Chaosreader predstavlja besplatni alat za praćenje TCP i UDP sesija te dohvaćanje podataka aplikacije iz *snoop* i *tcpdump* logova. Alat dohvaća telnet sesije, FTP datoteke, HTTP prijenose (poput HTML, GIF, JPEG itd.) te SMTP mailove iz logova mrežnog prometa.

Dnschef je alat pomoću kojeg se konfigurira „lažni“ DNS *proxy* za penetracijsko testiranje te analizu zlonamjernog softvera. DNS *proxy*, odnosno „lažni“ *proxy*, je alat koji se primjenjuje za analizu aplikacijskog mrežnog prometa. Može se koristiti za slanje lažnih

zahtjeva koji se mogu preusmjeriti na lokalni stroj za prekid ili presretanje prometa, umjesto na stvarni *host* negdje na Internetu, [28].

DSniff je alat za otkrivanje zaporki i analizu mrežnog prometa. Navedeni alat pasivno nadzire mrežni promet u potrazi za zanimljivim podacima poput zaporki, e-mailova, raznih datoteka itd.

Mitmproxy alat koristi se za otklanjanje pogrešaka, procjenu privatnosti te penetracijsko testiranje. Također, može se koristiti za presretanje, provjeru, izmjenu i reprodukciju web prometa poput HTTP/1 i HTTP/2, *WebSockets* ili bilo kojeg drugog SSL/TLS zaštićenog protokola, [29].

Tcpdump je alat za analizu paketa mrežnih podataka koji se pokreće preko sučelja s naredbenim retkom. Omogućava prikaz TCP/IP te drugih paketa koji se prenose kroz mrežu kako bi se riješili mrežni i sigurnosni problemi.

Wifite alat može se koristiti za napad na WEP, WPA i WPS kriptiranu mrežu. Sadrži razne značajke poput sortiranja mreža prema jačini signala, automatski odjavljuje klijente skrivenih mreža kako bi otkrio SSID-ove, mijenja MAC adrese prije izvršenja napada, sprema sve lozinke u tekstualnu datoteku te još mnoge druge značajke.

Wireshark jedan je od najpopularnijih alata na svijetu za analizu paketa mrežnog prometa. Upotrebljava se kako bi se riješili problemi te analizirala mreža i aplikacijski protokoli raznih tehnologija. Alat je besplatan te ima otvoreni kod, a dostupan je za Windows, Mac OS X, Linux te za nekoliko platformi sličnih Unix platformi. Pruža opsežne mogućnosti filtriranja, detaljne informacije o protokolu, statističke podatke te ugrađene značajke za analizu paketa kako bi se mogli identificirati i analizirati važni događaji u mreži, [30].

6. PROVEDBA FORENZIČKE ANALIZE MOBILNOG UREĐAJA

U ovom poglavlju bit će prikazana provedba forenzičke analize mobilnog uređaja pomoću Santoku Linux distribucije. Primijenit će se alati Santoku Linuxa namijenjeni za forenziku uređaja. Opisat će se cijeli postupak, počevši od same instalacije preko provođenja pripremnih radnji, ekstrakcije te analize podataka s mobilnog uređaja. Provodit će se forenzika mobilnog uređaja Samsung Galaxy J3. Temeljem provedene forenzičke analize ustanovit će se stvarne mogućnosti te funkcionalnosti alata za forenziku mobilnih uređaja primjenom Santoku Linux distribucije.

6.1. Instalacija Santoku Linuxa i pripremne radnje

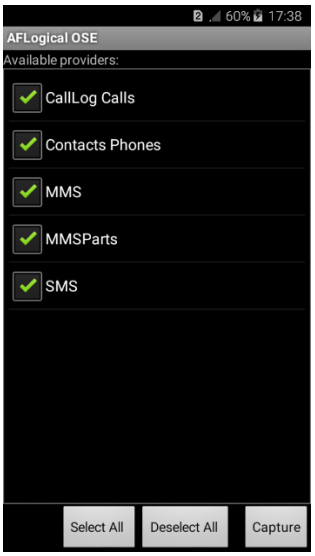
Preuzimanje instalacije Santoku Linux provodi se preko izvora [19], tj. preko internetske stranice Santoku Linux. U trenutku pisanja rada dostupna verzija distribucije je *Santoku 0.5*. Santoku Linux može se preuzeti kao ISO datoteka. Za potrebe ovog rada Santoku Linux distribucija instalirat će se kao virtualni stroj na *VMware Workstation Pro 16*. Instalacija navedene distribucije zahtijeva 64-bitni hardver za pokretanje, minimalno dvojezgreni procesor, 2 GB RAM memorije te minimalno 40 GB slobodnog prostora na tvrdom disku.

Prilikom instalacije potrebno je definirati naziv virtualnog stroja te definirati maksimalnu veličinu diska, RAM memoriju, broj jezgri procesora te ostale karakteristike hardvera kojima se konfigurira virtualni stroj. Pripremne radnje podrazumijevaju konfiguraciju Santoku Linuxa te povezivanje radne stanice s mobilnim uređajem. Za povezivanje radne stanice s mobilnim uređajem potreban je odgovarajući kabel, ovisno o proizvođaču i modelu mobilnog uređaja nad kojim će se provoditi forenzička analiza. Također, za pohranu ekstrahiranih podataka potrebna je SD kartica na koju će se podaci spremati.

6.2. Logička ekstrakcija podataka pomoću AF Logical OSE alata

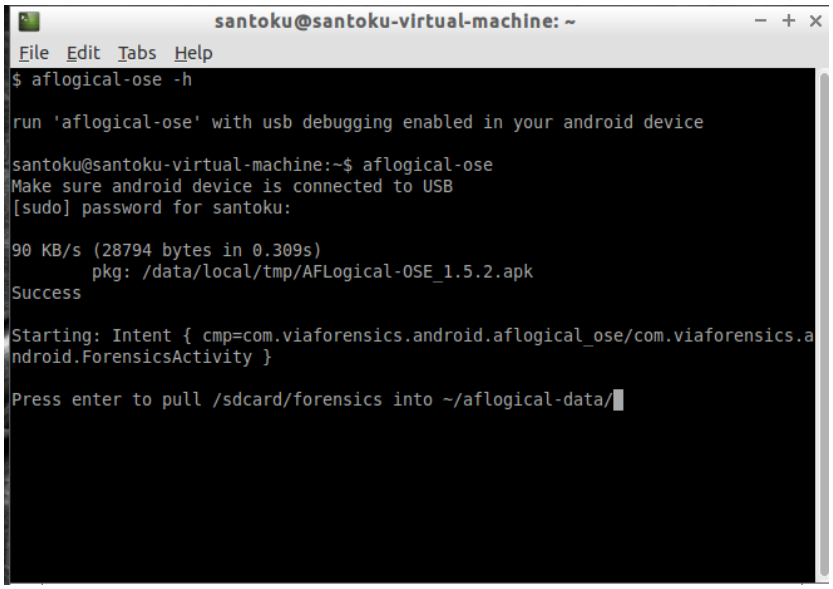
Kao što je već navedeno u prethodnom poglavlju, *AF Logical OSE* je alat koji se primjenjuje za logičku ekstrakciju podataka s mobilnog uređaja. Pomoću navedenog alata, moguće je ekstrahirati podatke poput logova poziva, SMS i MMS poruka, raznih datoteka, slika, video zapisa i slično. Za uspješnu primjenu *AF Logical OSE* alata potrebno je ostvariti prethodna dva koraka, a to su uspješna instalacija Santoku Linux distribucije te povezivanje mobilnog uređaja odgovarajućim kabelom na radnu stanicu. Zatim je potrebno omogućiti opciju *USB debugging* na mobilnom uređaju.

Sljedeći korak je pokretanje alata *AFLogical OSE* te unošenje u terminal sljedeće naredbe: *aflogical-ose*. Nakon toga potrebno je na mobilnom uređaju dozvoliti USB otklanjanje pogrešaka, tj. *USB debugging* prilikom čega je u obavijesti naveden RSA ključ računala koje pristupa mobilnom uređaju. Zatim se na ekranu mobilnog uređaja pojavi *AFLogical OSE* aplikacija unutar koje je potrebno odabrati koje podatke želimo ekstrahirati s mobilnog uređaja. Navedeni prikaz sa mobilnog uređaja prikazan je na slici 13.



Slika 13. *AFLogical* OSE na mobilnom uređaju

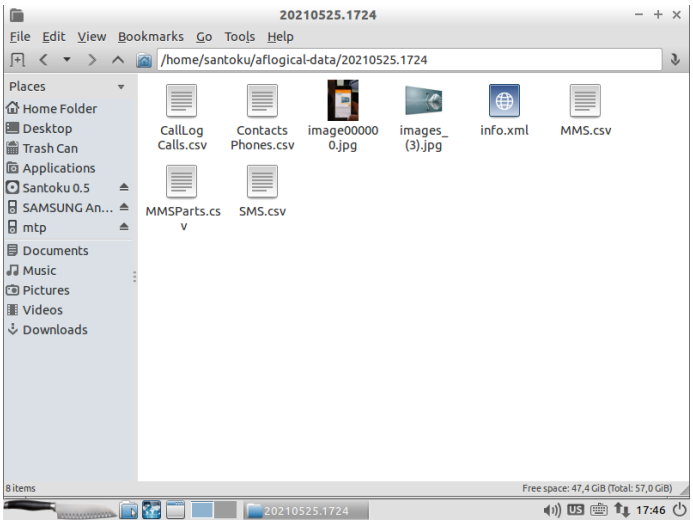
Nakon označavanja podataka koje želimo ekstrahirati te provedbe samog ekstrahiranja, podaci se pohranjuju u odgovarajuću mapu radne stanice. Na slici 14 prikazan je izgled terminala prilikom ekstrahiranja podataka pomoću Santoku Linux distribucije.



Slika 14. Pokretanje ekstrahiranja podataka kroz terminal

Ekstrahiranim podacima može se pristupiti unošenjem *cd* naredbe kroz terminal ili kroz *File Manager* otvaranjem mape pod nazivom *aflogical-data*. Unutar navedene mape nalaze se sljedeće datoteke kao što je to prikazano na slici 15:

- CallLog Calls.csv
- Contacts Phones.csv
- Info.xml
- MMS.csv
- MMSParts.csv
- SMS.csv.



Slika 15. Ekstrahirani podaci sa mobilnog uređaja

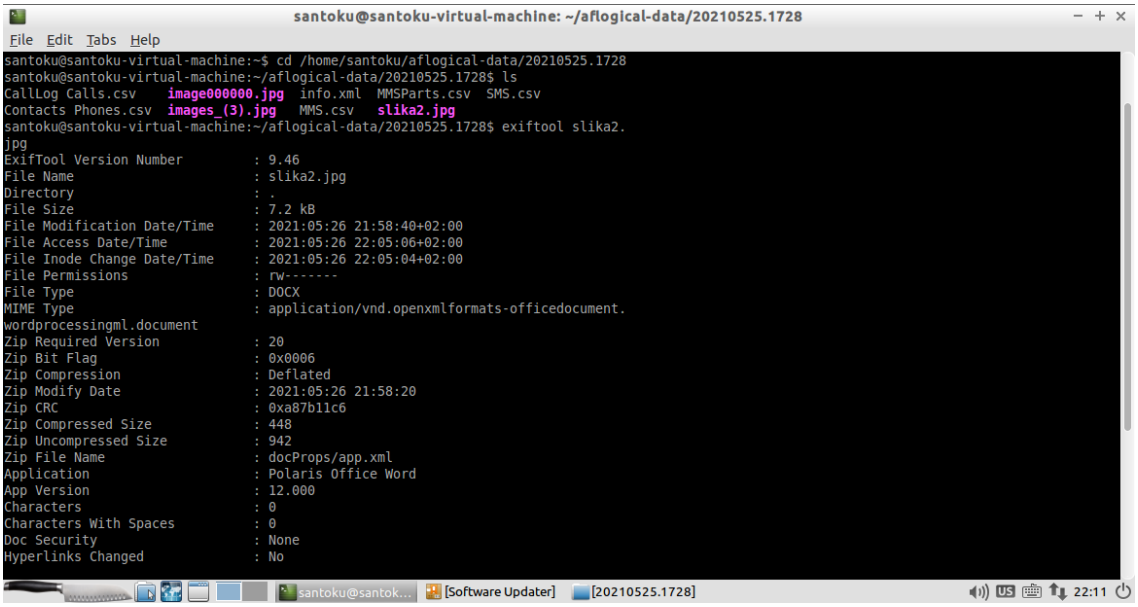
Unutar datoteke gdje su ekstrahirani logovi poziva vidljivi su sljedeći podaci: broj s kojeg je poziv upućen, tip poziva (odlazni ili dolazni), naziv kontakta, trajanje, datum, mjesto gdje je kontakt pohranjen te slični ostali podaci. Unutar *Contacts Phones.csv* datoteke nalaze se svi kontakti pohranjeni na mobilnom uređaju te brojevi tih kontakata, nazivi kontakata, koliko puta je upućen poziv prema tim kontaktima i slično. No, u ovoj datoteci nisu vidljivi kontakti koji su pohranjeni na SIM kartici mobilnog uređaja, već isključivo kontakti koji su pohranjeni na uređaju. U datotekama *SMS.csv* i *MMS.csv* nalaze se podaci o međusobno poslanim SMS i MMS porukama te detaljni podaci o tome kad je poruka poslana, tko ju je poslao, SIM IMSI od pošiljatelja, predmet i tijelo poruke, status, je li poruka pročitana i slično.

Ukoliko nakon provedene logičke ekstrakcije odabranih podataka želimo ukloniti *AFLogical OSE* aplikaciju s mobilnog uređaja, potrebno je unutar Santoku Linux terminala unijeti sljedeću naredbu*: sudo adb uninstall com.viaforensics.android.aflogical_ose*.

6.3. Primjena ostalih alata za forenziku mobilnog uređaja

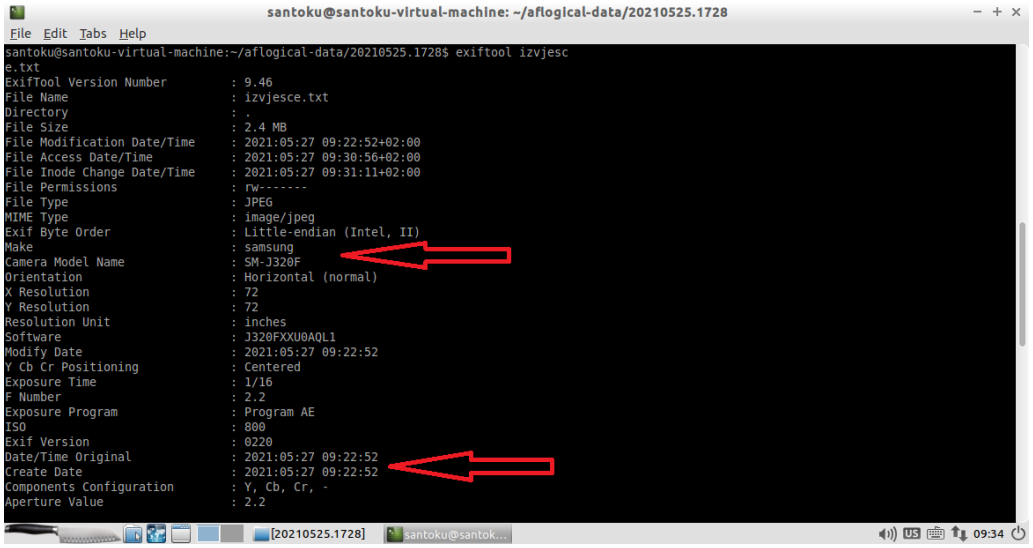
Sljedeći alat koji se koristi prilikom forenzičke analize mobilnog uređaja je *ExifTool*. Isti je primjenjiv za ekstrakciju metapodataka određenih slika, audio i video zapisa itd. Za

potrebe ispitivanja *ExifTool* alata, na mobilnom uređaju preko *File Manager* aplikacije promijenjena je ekstenzija tekstualne datoteke u JPG datoteku. Unosom naredbe *exiftool slika2.jpg* ekstrahirani su metapodaci navedene slike te je utvrđeno kako se ipak radi o DOCX tipu datoteke kao što je prikazano na slici 16.



Slika 16. Metapodaci datoteke *slika2.jpg*

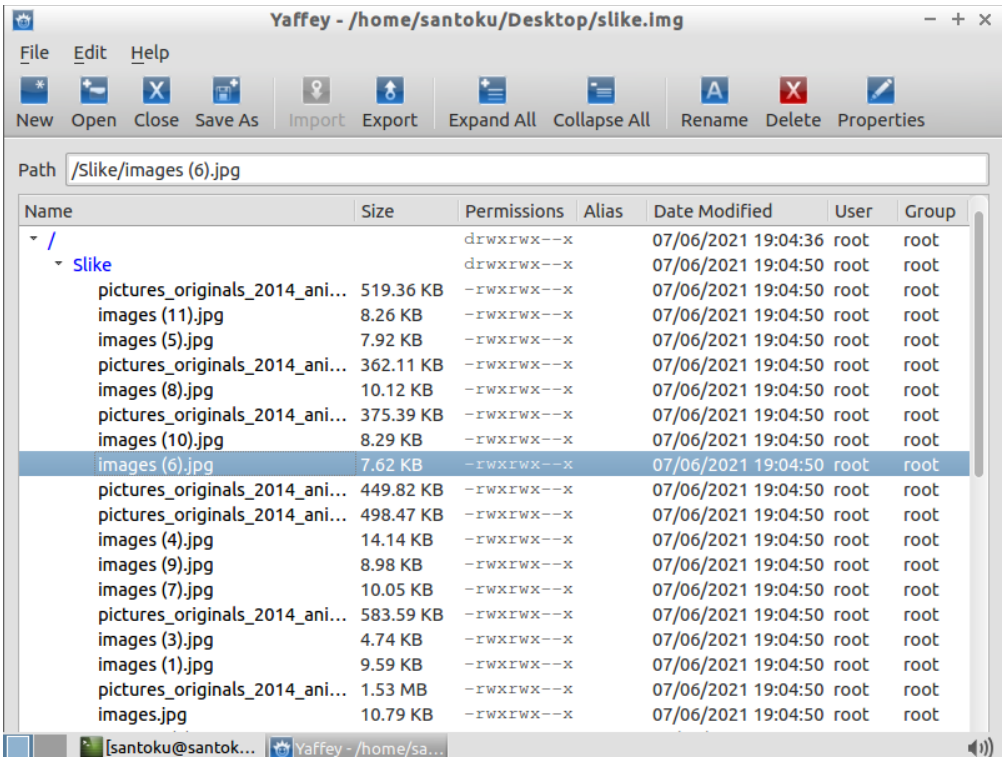
Upravo zbog mogućih razlikovanja ekstenzija i stvarnih tipova datoteka, unutar navedenih datoteka mogu se kriti određene poruke ili informacije. Takve informacije od velikog su značaja za cjelokupni postupak forenzičke istrage te je stoga *ExifTool* alat vrlo koristan. U obrnutom slučaju kada je ekstenzija JPEG datoteke promijenjena u TXT datoteku, također su vidljivi metapodaci. Na slici 17 prikazani su metapodaci iz kojih se vidi o kojem tipu datoteke se zapravo radi, podaci o proizvođaču i nazivu modela kamere, vremenu snimanja fotografije, ponekad i GPS koordinate mjesta snimanja fotografije te razni drugi metapodaci koji mogu biti od velike važnosti za forenzičku istragu.



Slika 17. Metapodaci o JPEG datoteci

Yaffey alat primjenjuje se za kreiranje novih YAFFS2 slika, otvaranje postojećih, uvoz ili izvoz datoteka ili mapa te razne druge funkcije. *Yet Another Flash Filing System* verzija 2 (YAFFS2) izdržljiv je i pouzdan datotečni sustav za pisanje koji se primjenjuje kod NAND i NOR *flash* uređaja. YAFFS2 nije dio glavnog stabla Linux kernela te zbog toga zahtijeva pribavljanje određenih izvora iz CVS repozitorija projekata kojim se zakrpa ciljani kernel izvor, [31].

Navedeni alat koristit ćemo za stvaranje YAFFS2 slike podataka mobilnog uređaja te za uređivanje stvorene slike podataka. Također, stvorenu sliku podataka možemo koristiti prilikom forenzičke analize i korištenja drugih alata unutar Santoku Linux distribucije. Na slici 18 prikazano je sučelje *Yaffey* alata unutar kojeg je otvorena novo kreirana slika *slike.img* unutar koje se nalaze određeni podaci i fotografije.

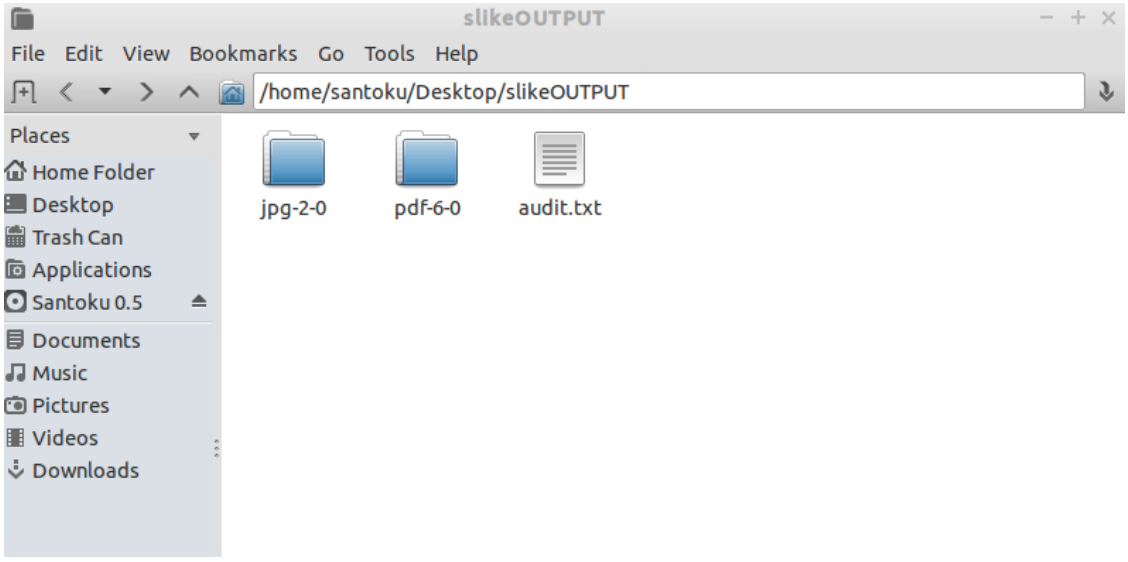


Slika 18. Sučelje *Yaffey* alata

Kao što je vidljivo s prikaza slike 18, otvorenu sliku moguće je uređivati na način da je moguće uvoziti/izvoziti podatke, moguće je preimenovati datoteke, urediti svojstva vezana za dozvole čitanja, pisanja i izvršavanja te određivanja vlasnika datoteke. Također, kreiranu YAFFS2 sliku podataka može se koristiti prilikom korištenja drugih alata kako bi došli do određenih podataka ili informacija bitnih za forenzičku istragu.

Scalpel alat vrši „rezbarenje“ datoteka na temelju uzoraka koji opisuju određeni tip datoteke ili fragmente određenih tipova datoteka. Navedeni uzorci mogu biti temeljeni na binarnim nizovima ili na regularnim izrazima. Komentari u konfiguracijskom dokumentu *Scalpel* alata opisuju formate rezbarenih uzoraka datoteka podržanih od strane alata. Na taj način može se unutar konfiguracijskog dokumenta alata označiti koje datoteke je potrebno oporaviti. Oporavljene datoteke pohranjuju se u zasebnu odgovarajuću mapu gdje se svrstavaju ovisno o tipu datoteke. Također, navedeni alat moguće je koristiti za oporavak svih izabranih datoteka hard diska.

Za potrebe ovog rada korišten je *Scalpel* alat za primjenu na kreiranoj YAFFS2 slici podataka pod nazivom *slike.img*. Unosom naredbe *sudo scalpel –c scalpel.conf –o slikeOUTPUT slike.img* kreirana je mapa *slikeOUTPUT*. Unutar mape pohranjeni su pronađeni podaci uz definirane određene parametre unutar konfiguracijskog dokumenta *scalpel.conf*. Prikaz mape slikeOUTPUT prikazan je na slici 19.



Slika 19. Prikaz prikupljenih datoteka pomoću *Scalpel* alata

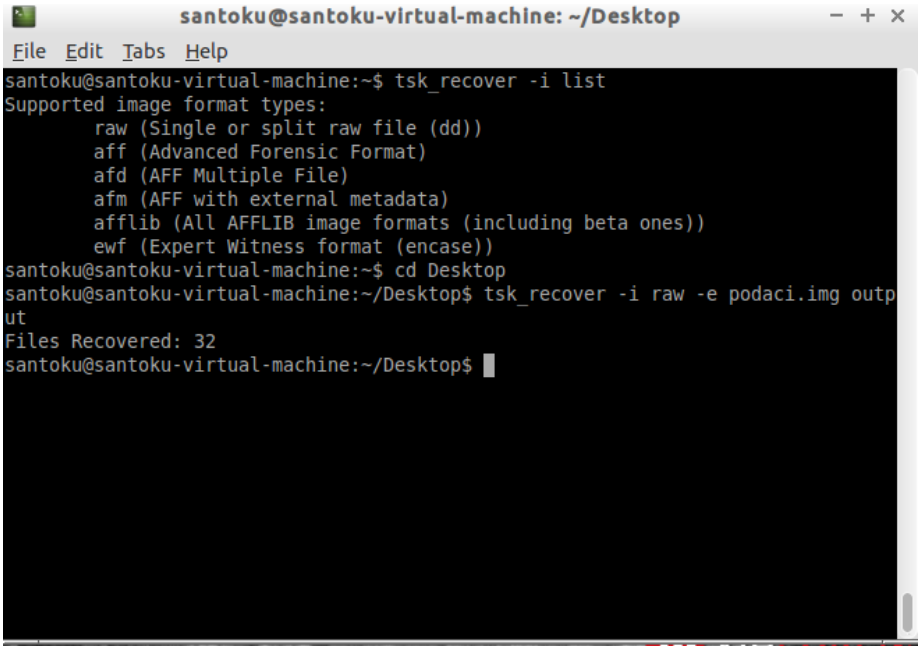
Iz slike 19 vidljivo je kako su prikupljene datoteke raspoređene unutar mapa koje nose naziv ovisno o tome o kojem tipu datoteke se radi. Također, uz te mape nalazi se *audit.txt* tekstualna datoteka koja sadrži zapis o vremenu pokretanja *Scalpel* alata, određene podatke o ekstrahiranim datotekama te podatak o vremenu završetka izvršenja unesene naredbe.

Android Brute Force Encryption alat koristi se za probijanje PIN-a kojim je zaključan mobilni uređaj. Uređaj je potrebno pokrenuti u *fastboot* modu, zatim *bootati* odgovarajuću sliku oporavka, tj. *recovery image*. Nakon toga potrebno je povući potrebne datoteke zaglavlja i podnožja kako bi mogli pokrenuti „*brute force*“ enkripcijskog PIN-a mobilnog uređaja. Prema zadanim postavkama testiraju se četveroznamenkaste numeričke zaporke. Navedeni proces pokreće se pomoću sljedeće naredbe: *bruteforce_stdcrypto ~/Desktop/tmp_header ~/Desktop/tmp_footer*.

Problem kod primjene ovog alata je taj što zahtijeva omogućenu opciju *USB debugging* do koje nije moguće doći standardnim postupkom ukoliko je mobilni uređaj

zaključan. Stoga je u ovom slučaju potrebna pomoć određenog drugog softverskog alata kojim bi se zaobišao zaključan uređaj te omogućila navedena opcija. Navedeno znatno otežava primjenu ovog alata.

SleuthKit alat može se primjenjivati u razne svrhe. Pomoću *SleuthKit* alata možemo provjeriti tip slike podataka te njenu veličinu. U našem slučaju radi se o *raw* tipu slike podataka. Također, pomoću navedenog alata moguće je vratiti izbrisane datoteke. Navedeno se izvršava pomoću *tsk_recover* naredbe pomoću koje se provodi oporavak izbrisanih datoteka. U našem slučaju proveli smo oporavak izbrisanih datoteka te su oporavljene 32 datoteke. Na slici 20 prikazano je izvršenje naredbe za oporavak podataka: *tsk_recover –i raw –e podaci.img output.* Navedenom naredbom definiran je oporavak podataka sa slike podataka *raw* tipa, uključujući sve datoteke (alocirane i nealocirane) sa slike podataka pod nazivom *podaci.img.* Naredbom je definirano spremanje oporavljenih podataka u mapu *output*.



Slika 20. Oporavak podataka pomoću alata *SleuthKit*

SleuthKit alat podržava razne oblike datotečnih sustava kao što su: NTFS, FAT, ExFAT, UFS 1, UFS 2, EXT2FS, EXT3FS, Ext4, HFS, ISO 9660 i YAFFS2. Alat se može pokrenuti na Windows i Unix operativnim sustavima.

Prilikom provedbe forenzičke analize mobilnog uređaja korišteni su razni alati čije su funkcionalnosti prikazane tablicom 1.

Tablica 1. Prikaz funkcionalnosti korištenih alata

Alat	**Funkcionalnosti**
AFLogicalOSE	Ekstrakcija logova poziva, kontakata uređaja, podataka o SMS i MMS porukama
ExifTool	Ekstrakcija metapodataka kao što su: tip datoteke, proizvođač mobitela, model kamere kojim je snimljena fotografija, datum i vrijeme snimanja fotografije, datum zadnje modifikacije
Yaffey	Kreiranje i uređivanje podataka koji su u obliku YAFFS2 slike podataka
Scalpel	Prikupljanje i oporavak datoteka raznih formata
SleuthKit	Oporavak izbrisanih datoteka sa raznih datotečnih sustava

Korišteni alati omogućuju ekstrakciju i oporavak raznih vrsta podataka. Pomoću *SleuthKit* alata uspješno su oporavljene izbrisane datoteke, dok su pomoću *ExifTool* alata ekstrahirani razni metapodaci te otkriven stvarni tip datoteka. Navedeno dokazuje kako su alati Santoku Linux distribucije funkcionalni, ali isto tako njihova primjena zahtijeva određenu razinu poznavanja njihovih mogućnosti. Količina podataka ekstrahirana alatima Santoku Linux distribucije odgovara razini logičke ekstrakcije podataka.

7. ZAKLJUČAK

Mobilni uređaji u današnje vrijeme predstavljaju vrlo značajan izvor informacija. Većina komunikacija odvija se putem mobilnih uređaja, čime oni postaju vrlo značajni forenzičkim istražiteljima. Pomoću forenzičke analize mobilnog uređaja može se doći do raznih podataka kao što su logovi poziva, poslane poruke, izbrisani podaci i fotografije te razni drugi podaci koji se uz legalne postupke mogu predočiti kao oblik digitalnog dokaza u mogućim sudskim procesima. Postoje razni tipovi ekstrakcije podataka koji ovisno o složenosti i vremenu potrebnom za izvršavanje mogu prikupiti veći ili manji broj potrebnih podataka. Ručna ekstrakcija podataka zahtijeva najmanje vremena i stručnog znanja, dok fizička ekstrakcija zahtijeva stručno znanje te više vremena za njenu provedbu, ali i daje najviše ekstrahiranih podataka kao rezultat cijelog procesa.

Santoku Linux distribucija može se primjenjivati za forenzičku analizu mobilnih uređaja, penetracijsko testiranje te ispitivanje mobilnih zlonamjernih softvera. Primjenom alata unutar Santoku Linux distribucije utvrđeno je kako postoji vrlo veliki broj korisnih alata za različite svrhe. Upotrebom alata za forenzičku analizu provedeno je prikupljanje podataka logičkom ekstrakcijom te su uspješno prikupljeni logički podaci s mobilnog uređaja. Također, uspješno se mogu ekstrahirati metapodaci slika, audio i video zapisa pomoću *ExifTool* alata. Jedan od značajnijih alata svakako je *SleuthKit* pomoću kojeg se mogu uspješno oporaviti izbrisane datoteke. Oporavak izbrisanih datoteka vrlo je važna funkcionalnost zbog toga što se forenzički istražitelji vrlo često susreću s mobilnim uređajima na kojima je potrebno oporaviti određene datoteke koji su ključni digitalni dokazi za forenzičku istragu. Navedeni alati samo su jedan dio alata korištenih u provedbi forenzičke istrage.

Problem prilikom korištenja određenih alata unutar Santoku Linux distribucije može izazvati zaključan mobilni uređaj. U tom slučaju moraju se tražiti drugi alati ili metode za omogućavanje razvojnog moda, odnosno *USB debugging* opcije. Prilikom logičke ekstrakcije podataka pomoću *AFLogical OSE* alata nisu prikazani kontakti koji su pohranjeni isključivo na SIM kartici, što je također jedan od nedostataka. Provedbom logičke ekstrakcije možemo zaključiti kako Santoku Linux distribucija zadovoljava potrebe s velikim brojem raznih alata. Pomoću navedene distribucije i alata *AFLogical OSE* provodi se logička ekstrakcija podataka

kojom se ne prikupljaju podaci koji su izbrisani te podaci s dijela memorije koji nije dodijeljen. Također, nije moguće zaobići zaključan ili zaštićen uređaj. Za probijanje PIN-a zaključanog uređaja moguće je iskoristiti *Android Brute Force Encryption* alat, dok je za oporavak izbrisanih datoteka moguće iskoristiti *SleuthKit* alat. Prednosti korištenja Santoku Linux distribucije su jednostavnost, kratko trajanje samog procesa ekstrakcije te velik izbor softverskih alata sadržanih u samoj distribuciji.

U konačnici možemo zaključiti kako Santoku Linux distribucija zadovoljava s brojem raznolikih alata, ali isto tako u daljnjim verzijama distribucije trebalo bi se poraditi na uklanjanju postojećih nedostataka te unaprjeđenju mogućnosti vezanih za logičku ekstrakciju podataka.

LITERATURA

[1] Kävrestad J. Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications. Skövde, Švedska: School of Informatics, University of Skövde; 2020.

[2] Husnjak, S. Autorizirana predavanja, kolegij Forenzička analiza informacijsko komunikacijskog sustava – Osnove digitalnih dokaza (2020/21); Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2020.

[3] Casey, E. Handbook of Digital Forensics and Investigation. San Diego, California, SAD; 2010.

[4] Statista portal. Preuzeto sa: https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/#:~:text=In%202020%2C%20the%20number%20of,projected%20to%20reach%207.41%20billion [Pristupljeno: kolovoz 2021.].

[5] Tahiri, S. Mastering Mobile Forensics. Birmingham, Ujedinjeno Kraljevstvo; 2016.

[6] Ayers, R., Brothers S., Jansen W. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101, Revision 1, SAD, 2014.

[7] Murphy, C.A.: Developing Process for Mobile Device Forensics, 2011.

[8] Arnes, A.: Digital Forensics. Norveška, 2018.

[9] Cellebrite. Preuzeto sa: https://www.cellebrite.com/en/platforms/ [Pristupljeno: kolovoz 2021.]

[10] MSAB. Preuzeto sa: https://www.msab.com/products/ [Pristupljeno: kolovoz 2021.]

[11] Oxygen Forensics. Preuzeto sa: https://www.oxygen-forensic.com/en/ [Pristupljeno: kolovoz 2021.]

[12] Herman M., Iorga M., Salim A.M., Jackson R.H., Hurst M.R., Leo R., Lee R., Landreville N.M., Mishra A.K., Wang Y., Sardinas R. NIST Cloud Computing Forensic Science Challenges, SAD; 2020.

[13] Stoyanova M., Nikoloudakis Y., Panagiotakis S., Pallis E., Markakis E.K. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. 2020;20(2):1-7

[14] Tamma R., Skulkin O., Mahalik H., Bommisetty S. Practical Mobile Forensics: Fourth Edition. Birmingham, Ujedinjeno Kraljevstvo; 2020.

[15] AvailForensics. Preuzeto sa: https://www.availforensics.com/AF-UFED-CAM [Pristupljeno: kolovoz 2021.]

[16] Bommisetty S., Tamma R., Mahalik H. Practical Mobile Forensics: Second Edition. Birmingham, Ujedinjeno Kraljevstvo; 2014.

[17] SecurityLearn. Preuzeto sa: http://www.securitylearn.net/tag/android-passcode-bypass/ [Pristupljeno: kolovoz 2021.]

[18] Afonin O., Katalov V. Mobile Forensics – Advanced Investigative Strategies. Birmingham, Ujedinjeno Kraljevstvo; 2016.

[19] Santoku. Preuzeto sa: https://santoku-linux.com/about-santoku/ [Pristupljeno: kolovoz 2021.]

[20] Parasram, S.V.N. Digital Forensics with Kali Linux. Birmingham, Ujedinjeno Kraljevstvo; 2017.

[21] Reddy N. Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations. Indija; 2019.

[22] Almusallam, A.M. Penetration Testing for Android Applications with Santoku Linux. Politehničko sveučilište Kalifornijskog fakulteta u Pomoni; 2018.

[23] Android Developers. Preuzeto sa: https://developer.android.com/studio/command-line [Pristupljeno: kolovoz 2021.]

[24] Eclipse Foundation. Preuzeto sa: https://www.eclipse.org/tools/eclipsetools-charter.php#:~:text=The%20Eclipse%20Tools%20Top%20Level,components%20for%20the%20Eclipse%20Platform. [Pristupljeno: kolovoz 2021.]

[25] Birani B., Birani M. iOS Forensics Cookbook. Birmingham, Ujedinjeno Kraljevstvo; 2016.

[26] Libimobiledevice. Preuzeto sa: https://libimobiledevice.org/#features [Pristupljeno: srpanj 2021.]

[27] The Sleuth Kit. Preuzeto sa: https://www.sleuthkit.org/sleuthkit/desc.php [Pristupljeno: kolovoz 2021.]

[28] Kali Tools. Preuzeto sa: https://tools.kali.org/sniffingspoofing/dnschef [Pristupljeno: kolovoz 2021.]

[29] Mitmproxy. Preuzeto sa: https://mitmproxy.org/ [Pristupljeno: kolovoz 2021.]

[30] Baxter J.H. Wireshark Essentials. Birmingham, Ujedinjeno Kraljevstvo; 2014.

[31] Yaghmour K., Masters J., Ben-Yossef G., Gerum P. Building Embedded Linux Systems. SAD; 2008.

POPIS KRATICA

ADB	(Android Debug Bridge) softverski alat za komunikaciju s uređajem
API	(Application Programming Interface) softverski posrednik za omogućavanje komunikacije između dvije aplikacije
APK	(Android Package) datoteka Android paketa za distribuciju aplikacija
ASCII	(American Standard Code for Information Interchange) američki normirani kod za razmjenu informacija
BSD	(Berkeley Software Distribution) operativni sustav sličan Unixu
CAINE	(Computer Aided INvestigative Environment) distribucija bazirana na Ubuntu kreirana za potrebe digitalne forenzike
CSV	(Comma-separated Values) format tekstualnih datoteka
DEFT	(Digital Evidence and Forensics Toolkit) Linux distribucija za računalnu forenziku
eMMC	(embedded Multi-Media Controller) vrsta *flash* pohrane temeljene na MMC standardu
FTP	(File Transfer Protocol) standardni komunikacijski protokol za prijenos podatka s poslužitelja na klijente unutar računalne mreže
GIF	(Graphics Interchange Format) grafički format za razmjenu slika
GPS	(Global Positioning System) satelitski radionavigacijski sustav za određivanje položaja na Zemlji
GUI	(Graphical User Interface) grafičko korisničko sučelje
HD	(High Definition) visoka rezolucija slike ekrana
HTML	(HyperText Markup Language) prezentacijski jezik za izradu web stranica

HTTP	(Hypertext Transfer Protocol) protokol aplikacijskog sloja za prijenos hipermedijskih dokumenata
HTTPS	(Hypertext Transfer Protocol Secure) ekstenzija HTTP protokola za sigurnu komunikaciju
IMSI	(International Mobile Subscriber Identity) broj za jedinstvenu identifikaciju svakog korisnika ćelijske mreže
iOS	(iPhone Operating System) mobilni operativni sustav razvijen od tvrtke Apple
IoT	(Internet of Things) sustav međusobno povezanih računalnih uređaja
ISP	(Internet Service Provider) pružatelj usluge Interneta
JPEG	(Joint Photographic Experts Group) standardni format slika
JTAG	(Joint Test Action Group) industrijski standard za provjeru dizajna i ispitivanje tiskanih pločica
LAN	(Local Area Network) lokalna računalna mreža unutar ograničenog područja
M2M	(Machine to Machine) izravna komunikacija između uređaja
MAC	(Media Access Control) jedinstveni identifikator mrežne kartice
MMS	(Multimedia Messaging Service) standard za slanje multimedijskog sadržaja kroz ćelijsku mrežu
NIST	(National Institute of Standards and Technology) Nacionalna ustanova za norme i tehniku
PCB	(Printed Circuit Board) pločica za spajanje elektroničkih komponenata
PDF	(Portable Document Format) format datoteke za prezentaciju dokumenata
PIN	(Personal Identification Number) lozinka za zaštitu pristupa uređaju
RAM	(Random-access memory) oblik računalne memorije čijem se sadržaju može izravno pristupiti

RSA	(Rivest-Shamir-Adleman) kripto sustav s javnim ključem koji se koristi za siguran prijenos podataka
SANS	(SysAdmin, Audit, Network and Security) institut za obuku, istraživanje i certificiranje u području kibernetičke sigurnosti
SD	(Secure Digital) memorijske kartice za pohranu podataka
SDK	(Software Development Kit) skup alata za razvoj softvera
SIM	(Subscriber Identity Module) čip za pohranu informacija važnih za komunikaciju s mobilnim ćelijama operatera
SMS	(Short Message Service) usluga slanja tekstualnih poruka
SMTP	(Simple Mail Transfer Protocol) internetski standardni komunikacijski protokol za prijenos elektroničke pošte
SSD	(Solid State Drive) neizbrisiva memorija za pohranu podataka
SSID	(Service Set Identifier) naziv bežične mreže
SSL	(Secure Sockets Layer) standardna tehnologija za zaštitu internetske veze i podataka koji se razmjenjuju između sustava
TCP	(Transmission Control Protocol) transportni protokol za osiguranje pouzdanog prijenosa podataka
TLS	(Transport Layer Security) kriptografski protokol za pružanje sigurne komunikacije putem računalne mreže
TXT	(TeXT) standardni tekstualni dokument
UDP	(User Datagram Protocol) protokol za prijenos podataka koji pruža mogućnost otkrivanja oštećenih podataka unutar paketa
UFED	(Universal Forensic Extraction Device) alat za ekstrakciju fizičkih i logičkih podataka s mobilnih uređaja

USB	(Universal Serial Bus) standard za uspostavljanje specifikacija za kabele i konektore, te protokole za povezivanje, komunikaciju i napajanje
Wi-Fi	(Wireless Network Technology) bežična mrežna tehnologija za povezivanje na Internet

POPIS SLIKA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

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

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

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Forenzika mobilnog uređaja primjenom distribucije Santoku Linux**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 20.8.2021

(potpis)