Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.42:004.738.12
DOI: https://doi.org/10.24867/16BE07Antesevic

АНТИФОРЕНЗИКА МОБИЛНИХ УРЕЂАЈА

MOBILE ANTI-FORENSICS

Светлана Антешевић, *Факултет техничких наука, Нови Сад*

Област: ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду обрађена је антифорензика мобилних уређаја. Разматране су и анализиране технике везане за антифорензику мобилних уређаја и представљени су и детаљно описани алати који имплементирају те технике. Акценат је стављен на обраду техника и алата везаних за iOS и Android оперативни систем због њихове доминантности на тржишту.*

Кључне речи: *дигитална форензика, антифорензика, iOS, Android, технике, алати*

Abstract – *This paper addresses the anti-forensics of mobile devices. Techniques related to anti-forensics of mobile devices are considered and analyzed, and tools that implement these techniques are presented and described in detail. Emphasis is placed on the processing of techniques and tools related to the iOS and Android operating systems due to their dominance in the market.*

Keywords: *digital forensics, anti-forensics, Android, iOS, techniques, tools*

1. УВОД

Током протеклих година, сведоци смо све веће распрострањености мобилних уређаја широм света. Не само да број корисника расте, него се и уређаји све више користе за низ свакодневних активности. То указује на све већи број нелегалних радњи који се обављају путем мобилних уређаја. Такође, са жељом да се сакрију, уклоне или униште подаци који могу бити мета или разлог неког напада, спроводе се разне активности како би се докази који су ускладиштени у мобилном уређају уништили, компромитовали или избрисали тј. како би се онемогућила форензичка истрага. Стога, циљ овог рада јесте да се истраже и презентују антифорензичке технике и алати код мобилних уређаја како би се потпомогао процес форензичке истраге мобилних уређаја, дала ближа слика антифорензичких метода над мобилним уређајима и како би се открили или ближе представиле легалне и нелегалне радње над мобилним уређајима.

Друго поглавље овог рада бави се прегледом области из дигиталне форензике, објашњени су основни појмови везани за форензику мобилних уређаја, архитектуру и безбедносне механизме самих мобилних уређаја, појмове везане за дигиталну антифорензику и антифорензику мобилних уређаја. У трећем поглављу размотрене су и детаљно анализиране опште технике код дигиталне антифорензике као и антифорензичке технике код мобилних уређаја са *iOS* и *Android* оперативним системом. Кроз четврто поглавље дат је приказ тренутно коришћених алата који се користе ради примене антифорензичких метода током процеса истраге или ради детектовања спроведених антифорензичких метода над мобилним уређајем.

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Стеван Гостојић, ванр. проф.

2. ПРЕГЛЕД ОБЛАСТИ

2.1. Дигитална форензика

Дигитална форензика је употреба научно изведених и проверених метода за очување, прикупљање, проверу ваљаности, идентификацију, анализу, тумачење, документацију и презентацију дигиталних доказа изведених из дигиталних извора у сврху олакшавања или унапређења реконструкције догађаја за које се утврди да су кривични или да помажу да предвиди неовлашћене радње за које се показало да ометају планиране операције [1]. Разноликост различитих уређаја, оперативних система и софтвера довела је до потребе да се дигитална форензика подели на више подобласти у зависности од врсте уређаја. Области дигиталне форензике представљају: форензика рачунара, форензика рачунарских мрежа, форензика мобилних уређаја, форензика мултимедијалних записа и остало (нпр. уграђени системи, IoT, облак итд.). Дигитална форензичка истрага се састоји од шест фаза, а то су: идентификација, прикупљање, чување, прегледање, анализа и презентација доказа.

2.2. Форензика мобилних уређаја

Форензика мобилних уређаја је област дигиталне форензике чији предмет су докази ускладиштени на мобилним уређајима или преношени преко целуларне мреже [2]. Целуларна (мобилна) мрежа представља јавну комуникациону мобилну мрежу за пренос говора, текстуалних порука и података.

Мобилни уређаји су незаобилазно средство у свакодневном животу појединаца. Намењени за комуникацију и коришћење разних сервиса и са собом носе мноштво података о корисницима. Као такви, постају главна мета разних злоупотреба и криминалних активности због података који су у њима похрањени. Како на тржишту последњих година преовлађују два оперативна система *iOS* и *Android*, у наставку ће бити разматрана ова два оперативна система.

iOS је мобилни оперативни систем развијен и дистрибуиран од стране *Apple* компаније. Универзалан је оперативни систем за све *Apple* уређаје као што су

Apple TV, iPad, iPod Touch и *iPhone*. На тржишту мобилних уређаја представља удео од отприлике 26% [3]. Управља хардвером уређаја и пружа технологије потребне за имплементацију нативних апликација. iOS архитектура се састоји од четири слоја: *cocoa touch, media layer, core services layer* и *core OS layer.*

Android је оперативни систем за мобилне уређаје. Представља пројекат отвореног изворног кода. На тржишту мобилних уређаја заузима највећи удео, око 70% [3]. Постоји више дистрибуција *Android* платформе од стране различитих произвођача (*LG, Samsung, Huawei* итд.) који користе различите хардверске архитектуре и различите продавнице апликација. *Android* архитектура се састоји од различитих слојева [4]: *Linux Kernel, hardware abstraction layer, android runtime, native C/C++ library u java API framework.*

Мобилна безбедност или тачније безбедност мобилних уређаја, је области информационе безбедности која се бави заштитом паметних телефона, таблета и преносних рачунара од претњи. Посебно забрињава сигурност личних и пословних података који се сада чувају на паметним телефонима. Постоје добре праксе које треба поштовати на свим нивоима, од дизајна до употребе, преко развоја оперативних система, слојева софтвера и апликација за преузимање [5].

iOS је дизајниран са безбедношћу у својој основи и са више слојева сигурности. Хардверске функције ниског нивоа штите од напада злонамерног софтвера, а функције високог нивоа оперативног система спречавају неовлашћену употребу [6]. *Android* је дизајниран са посебним фокусом на безбедност. *Android* као платформа нуди и примењује одређене функције које штите корисничке податке присутне на мобилном уређају кроз вишеслојну сигурност.

Постоје одређене подразумеване поставке безбедности које ће заштитити корисника и одређене понуде које развојна заједница може да искористи за изградњу сигурних апликација.

2.3. Дигитална антифорензика

У овом раду ћемо се служити дефиницијом да је антифорензика процес компромитовања доступности, поузданости и корисности доказа током процеса форензичке истраге [7]. То су покушаји да се негативно утиче на постојање, количину и/или квалитет доказа са места злочина или да се отежа или онемогући прегледање и анализа доказа [8].

Дигитална антифорензика има широк спектар области примене и сврхе. Постоје одређени индикатори који дигиталним форензичарима могу помоћи у откривању таквих намера.

Неки од њих су: шифровани подаци на уређају, докази о брисању артефаката, докази о скривању трагова, присуство антифорензичких алата и слично.

3. ТЕХНИКЕ АНТИФОРЕНЗИКЕ

Антифорензичке технике постају велика препрека за дигиталну форензичку заједницу. Многе од техника представљају значајне изазове и могу онемогућити опоравак података користећи типичне форензичке праксе.

3.1. Антифорензичке технике

Генерално идентификоване антифорензичке технике описане су у наставку овог одељка.

Скривање доказа (енг. *hiding evidence*) представља радње које су преузете ради смањења или чак поништавања доступности доказа током форензичке истраге.

Шифровање је процес кодирања информација у коме се отворени текст трансформише у шифрат тако да само ауторизоване особе, које поседују криптографски кључ, могу да дешифрују шифрат.

Стеганографија је процес скривања једне поруке у другој поруци која може бити у облику текста, фотографије, видеа или аудио снимка.

Контрацепција података укључује антифорензичке технике које не производе доказе или производе мало дигиталних доказа. Оне се односе на посредно позивање системских функција, инјекцију удаљених библиотека, директну манипулацију објектима језгра оперативног система и преносне апликације.

Манипулација чврстим диском односи се на скривање партиција на диску.

Манипулација системом датотека представља скривање датотека или директоријума у систему датотека.

Скривање у меморији је скривање података у радној меморији уређаја.

Скривање података на мрежи укључује антифорензичке технике као што су *proxy* сервери, виртуалне приватне мреже (*virtual private network - VPN*) итд.

Брисање артефаката (енг. *artifact wiping*): Укључује антифорензичке технике које свесно уништавају доказе како би били неупотребљиви током истражног процеса. *Техника размагнетисања диска* је процес демагнетизирања ради уништавања података похрањених на чврстим дисковима и другим магнетним медијумима. *Брисање чврстог диск*а је потпуно брисање свих података са диска. *Уништавање датотека* је процес који укључује сигурно брисање рачунарске датотеке. *Уништавање метаподатака датотека* је брисање информација о другим подацима. *Брисање регистара* подразумева брисање кључа или ставке регистратора. *Брисање лог датотека* представља трајно брисање лог датотека са диска. *Брисање спољашњих медијума* представља брисање података на преносивим дисковима попут USB меморијског стика. *Генеричко брисање података* су технике и алати који могу да изврше више од једног типа брисања података.

Скривање трагова (енг. *trail obfuscation*) представљају антифорензичке технике које намерно дезоријентишу и преусмеравају форензичку истрагу.

Промена backbone мреже представља повезивање основне мреже са различитим мрежама и подмрежама ради размене информација између њих.

Лажирање IP адресе подразумева коришћење неколико *IP* адреса ради прикривања стварне *IP* адресе.

Лажирање MAC адресе је мењање хард кодираног броја *MAC* адресе повезаног са својом мрежном картицом.

Манипулација лог датотекама представља мењање лог датотека, временских линија активности и догађаја који су се догодили.

Коришћење proxy сервера представља. коришћење серверске апликације која служи као посредник између клијената који захтева ресурс и сервера који пружа тај ресурс.

Погрешно усмеравање података је преношење истинитих података преко лажних „тајних“ података.

Тројанске команде представљају злонамеран софтвер који је дизајниран да оштети, омета и уради податке.

Напад на форензичке технике и алате (енг. *attacks on forensics methods and tools*) укључује антифорензичке технике које подразумевају нападе на софтверске алате који се користе у форензичким истрагама и на технике које ти алати имплементирају. У ове нападе спадају: упозорења за употребу форензичких алата, технике против реверзног инжењеринга, напад на интегритет форензичког софтвера, напади на интегритет *hash* вредности, напади на интегритет истражитеља и програмски пакери.

Уклањање извора доказа (енг. *eliminating evidence sources*) представља неутрализацију извора доказа. Ова техника се не тиче уништавања већ спречавања стварања доказа.

Фалсификовање доказа (енг. *counterfeiting evidence*) представља стварање лажне верзије доказа који је правилно направљен да носи погрешне информације како би се преусмерио судски поступак.

3.2. Антифорензичке технике Android-а

Неке од антифорензичких технике које су везане за *Android* платформу су описане у овом одељку.

Техника искоришћавања *Android* функција односи се на управљање различитим дозволама за датотеке на нивоу оперативног система омогућавајући тиме спровођење тих функција.

Уништавање доказа ускладиштених на *Android* уређајима односи се на брисање повезаних база података како би се трајно избрисали одговарајући подаци. Углавном се спроводи путем одговарајућих алата за брисање.

Скривање доказа ускладиштених на *Android* уређајима односи се на чување доказа у приватној фасцикли. Приватна фасцикла је директоријум који је недоступан за било које друге апликације. Може служити за складиштење било које врсте информација, које су невидљиве за крајњег корисника и подаци нису приступачни унутар ње.

3.3. Антифорензичке технике iOS-а

Антифорензичке технике код *iOS* уређаја своде се на прикривање, брисање или уметање података како би се отежала форензичка истрага.

Брисање датотека на iOS-у је примена стандардних техника брисања метаподатака и података како би се отежао процес форензичке истраге.

Техника прикривања која побољшава сигурност незаштићених података који мирују на *iOS* уређајима осмишљена да учини садржај нечитким без одговарајућег 256-битног кључа. Инспирисана је шифром са случајним кључем (енг. *one-time pad - OTP*) коју је дизајнирао *Gilbert Vernam 1917.* [9].

4. АЛАТИ

У оквиру овог одељка представљени су алати који се користе за антифорензичку анализу мобилних уређаја. Алати који су истражени сортирани су по техникама које примењују.

4.1. Алати за скривање доказа

Cyphertop је алат за шифровање података који се користи и на *iOS*-у и на *Android*-у. Користи симетрични систем шифровања по блоковима. Поседује скривена складишта за чување шифрованих података, нуди стеганографске функције скривања података, нуди функције потпуног скривеног разговора.

Orbot Proxy with TOR представља бесплатну *proxy* апликацију која користи *TOR* за шифровање интернет саобраћаја.

K-9 Mail sa APG представља апликацију која шифрује е-пошту на *Android* уређају.

EncriptRIGHT представља алат који врши маскирање података на начин који одговара сваком кориснику који је овлашћен да приступи осетљивим подацима и да их заштити од безбедности ради примене одговарајуће приватности података.

StegDroid Alpha је једноставна апликација која се може користити за скривање текстуалних порука унутар аудио датотека, применом стеганографије.

PixelKnot апликација користи стеганографски алгоритам F5 који имплементира матрично кодирање ради побољшања ефикасности уграђивања и користи пермутације како би равномерно распоредио промене по целом стеганограму.

Da Vinci Secret Image преставља апликацију која се користи ради сакривања тајне поруке унутар слике.

Rootkit програм који је написан за *Android* платформу може се активирати путем телефонских позива или *SMS*-а када се инсталира на телефон, дајући криминалцима прикривен и тешко уочљив алат за пребацивање података са телефона или погрешно усмеравање корисника.

4.2. Алати за брисање доказа

Blancco Mobile Solutions омогућава трајно брисање свих података са паметних телефона и таблета који раде на различитим оперативним системима.

BatchPurifier је алат за уклањање скривених података и метаподатака из више датотека.

Неки од алата за брисање податка који трајно ресетују мобилне уређаје су: *BitRaser, Dr.Fone - Data Eraser (Android), Coolmuster Android Eraser, MobiKin Android Data Eraser.*

Vipre Android Security је алат који даје могућност праћења безбедности *Android* уређаја, праћење где се налази уређај и даљинског брисања података са уређаја.

4.3. Алати за детектовање антифорензичких поступака

XRY је софтверски алат компаније *MSAB* за прикупљање дигиталних доказа из мобилних уређаја. Садржи функционалности које могу да детектују злонамерни софтвер, обрисане податке из облака и резервних копија.

Anti-malware SDK for Android може се користити за скенирање злонамерног софтвера у било којој врсти *Android* датотеке.

The Zimperium Mobile Threat Defense (MTD) платформа пружа континуирано праћење и анализу на уређају за откривање мобилних напада у реалном времену.

Oxygen Forensics Mobile је софтвер који омогућава преузимање података са нових уређаја, приступ сигурнијим подацима и обнављања избрисаних записа. Проналази лозинке за шифроване резервне копије и слике уређаја.

MOBILedit Forensic претражује, испитује и извештава о подацима са *GSM/CDMA/PCS* мобилних телефона. Додатне функције овог алата укључују услугу која омогућава приступ бази података *IMEI* за регистрацију и проверу украдених телефона.

5. ЗАКЉУЧАК

Како би се потпомогао процес форензичке истраге мобилних уређаја, дала ближа слика антифорензичких метода над мобилним уређајима и открило антифорензичке радње над мобилним уређајима, у овом раду су анализиране технике и алати који се користе у сврху компромитовања, брисања и уништавања доказа релевантних за форензичку истрагу.

Да би се превазишли проблеми који се јављају у форензици мобилних уређаја, неопходно је спровести даља истраживања из области антифорензике мобилних уређаја и било би пожељно направити базу података која садржи легалне и нелегалне антифорензичке технике над мобилним уређајима и списак алата који имплементирају те технике.

6. ЛИТЕРАТУРА

[1] André Årnes, *Digital Forensics*, First. John Wiley & Sons Ltd, 2018. [Online]. Available: https://lccn.loc.gov/2017004725

[2] Стеван Гостојић, "06 Форензика мобилних уређаја." 2021.

[3] "Mobile Operating System Market Share Worldwide," *StatCounter Global Stats*. https://gs.statcounter.com/os-market-share/mobile/worldwide (accessed Sep. 16, 2021).

[4] "Platform Architecture," *Android Developers*. https://developer.android.com/guide/platform (accessed Sep. 08, 2021).

[5] "Mobile security," *Wikipedia*. Aug. 18, 2021. Accessed: Sep. 08, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Mobile_security&oldid=1039460744

[6] *Read Practical Mobile Forensics Online by Satish Bommisetty, Rohit Tamma, and Heather Mahalik | Books*. Accessed: Sep. 08, 2021. [Online]. Available: https://www.scribd.com/book/272076743/Practical-Mobile-Forensics

[7] "Digital Forensics Explained," *Routledge & CRC Press*. https://www.routledge.com/Digital-Forensics-Explained/Gogolin/p/book/9780367503437 (accessed Sep. 08, 2021).

[8] Стеван Гостојић, "09 Антифорензика." 2021.

[9] C. DOrazio, A. Ariffin, and K.-K. R. Choo, "iOS Anti-forensics: How Can We Securely Conceal, Delete and Insert Data?," in *2014 47th Hawaii International Conference on System Sciences*, Jan. 2014, pp. 4838–4847. doi: 10.1109/HICSS.2014.594.

Кратка биографија:

Светлана Антешевић рођена је у Новом Саду 1997. године. Завршила је основну школу „Мирослав Антић" у Футогу и средњу школу „Светозар Милетић" у Новом Саду. Дипломирала је 2020. године на Факултету техничких наука у Новом Саду, смер Рачунарство и аутоматика, са темом „Имплементација сервисних модула без серверских конфигурација". Исте године је уписала мастер студије на смеру Рачунарство и аутоматика, модул Примењене рачунарске науке и информатика – Електронско пословање.