Дигитална форензика – правци развоја насупрот актуелној пракси

Милица Јанковић, Радован Радовановић, Никола Митровић, Милан Јовановић

***Апстракт* — Дигитална форензика представља најактуелнију грану форензике. Како се развија информатичка наука и технологија у целини, тако се и дигитална форензика мора развијати да би пратила трендове и дала решење за све проблеме у свом научном домену. У овом раду се приказују планиран напредак у оквиру ове науке, као и тренутни поступци у пракси, и даје се њихова упоредна анализа.**

***Кључне речи* — дигитална форензика, информатичке науке, технологија.**

I. Увод

Брзи напредак технологије променио је начин на који људи комуницирају, раде и манипулишу подацима, али и довео до повећања криминалитета и све већег броја дигиталних злочина. Као резултат експанзије броја дигиталних уређаја и њихове употребе, трагови настали употребом ових уређаја постају све важнији у борби против криминала. На дигиталним уређајима могу се наћи подаци о вршењу кривичног дела путем алата за комуникацију, чувању информација о жртви, чувању доказа о извршењу неке криминале радње на уређају за складиштење података, подаци о друштвеним мрежама [1], базама података, подаци о историји претраживања итд. Све ове информације често су кључни докази у истрази и сврставају дигиталну форензику у једну од најзаступљенијих грана форензике 21. века.

Дигитална форензика се базира на употреби научно изведених и доказаних метода за очување, прикупљање, валидацију, идентификацију, анализу, интерпретацију, документацију и представљање дигиталних доказа изведених из дигиталних извора у сврху олакшавања или унапређења реконструкције догађаја за које се утврди да су криминални, или потпомаже у предвиђању криминалних радњи [2].

Према области испитивања дигиталну форензику можемо поделити на форензику рачунара, форензику мобилних уређаја, форензику софтвера, форензику Cloud окружења, мрежну и форензику база података [3,4], али и по компонентама (хардвер, софтвер, и услуге) [4]. Пандемија која је почела у 2020. години додатно је довела до убрзање дигитализације у друштву. Рад од куће постао је уобичајна ситуација која је повећала потражњу за дигиталним уређајима међу појединцима. Као последица повећаног обима коришћења различитих уређаја, али и времена проведеног на истим, велика количина информација о корисницима и њиховом животу се може наћи на тим уређајима [5]. Број случајева у којима су дигитални докази релевантни за истраге такође расте [6]. Велика количина и обим доступних података, са друге стране отежава ефикасност спровођења форензичке истраге.

Форензичка истрага дигиталних доказа је компликован процес који почиње на месту злочина, наставља се у форензичкој лабораторији ради истраге, а завршава се на суду где коначну пресуду доноси судија [3].

Иако у пракси традиционална форензика подразумева технике које се користе за прикупљање дигиталних доказа са медија за складишћење података, еволуција рачунарства довела је до пораста сајбер-злочина у Cloud окружењу. Данас већина компанија и организација свакодневно преноси своје производе и услуге преко Cloud окружења због вишеструких предности, укључујући мању цену IT инфраструктуре, континуитет пословања и приступ аутоматским ажурирањима. Међутим, безбедност у Cloud окружењу представља главну препреку за организације да пренесу своје системе на ову платформу. Штавише, пошто је форензичка истрага у Cloud окружењу сложена, безбедносни аналитичари виде рачунарство у Cloud окружењу као потенцијалну област забринутости.

Са увођењем рачунарства у Cloud окружењу, велики део хардвера који се односи на IT, као што су мрежни прекидачи, рекови и сервери, замењен је виртуелизованим софтвером на даљину на захтев који је конфигурисан у складу са пословним потребама. Осим тога, овим услугама и подацима може управљати и хостовати трећа страна или корисник са било ког места. Дакле, подаци и софтвер имају могућност да се физички складиште на више географских локација. Ова дистрибутивна природа података значајно смањује контролу и видљивост над дигиталним форензичким артефактима форензичким стручњацима. Слично, дигитални форензички алати и технике се обично разликују по цени, сложености и функционалности. Због

Милица Јанковић – Криминалистичко - полицијски универзитет, Цара Душана 196, 1100 Београд, Србија (e-mail: jankovicmilica095@gmail.com).

Радован Радовановић – Криминалистичко - полицијски универзитет, Цара Душана 196, 1100 Београд, Србија (e-mail: radovan.radovanovic@kpu.edu.rs).

Никола Митровић – Криминалистичко - полицијски универзитет, Цара Душана 196, 1100 Београд, Србија (e-mail: nikola.mitrovic@kpu.edu.rs) (https://orcid.org/0000-0001-5970-2654).

Милан Јовановић – Криминалистичко - полицијски универзитет, Цара Душана 196, 1100 Београд, Србија (e-mail: mjnmilan9@gmail.com).

 ISBN 978-86-7466-969-3

тога већина дигиталних форензичких алата садржи хетерогене делове или елементе, што повећава њихову некомпатибилност за заједнички рад. Штавише, неки форензички алати нису у стању да се носе са све већим капацитетом складиштења циљних уређаја. То значи да огромне мете представљају велики технички изазов за дигиталне форензичке операције јер захтевају сложеније технике анализе. Стога различити технички изазови представљају велику претњу перформансама и интегритету дигиталних форензичких операција [7].

II. Дигитални докази

Дигитални докази играју важну улогу у широком спектру кривичних дела и представљају дигиталне трагове који садрже доказне информације које се користе у судским процесима. Дигитални докази се могу лако модификовати, дуплирати или уништити, па је приликом предузимања истраге неопходно применити и одговарајуће алате који спречавају модификацију података. Циљ истражног процеса је прикупљање доказа коришћењем прихватљивих метода или процедура како би докази били прихватљиви и применљиви и на суду [3].

III. Фазе прикупљања и обраде дигиталних доказа у дигиталној форензици

А. Идентификација

Прва фаза дигиталног форензичког процеса је идентификација релевантних дигиталних доказа. Ово укључује идентификацију једног или више извора за складиштење дигиталних информација повезаних са истрагом. Неки од примера хардвера који може обезбедити дигиталне доказе укључују хард-дискове на рачунарским системима, меморијске картице, УСБ меморије, као и друге екстерне изворе, мобилне телефоне, интернет мрежу, и тако даље [2].

Б. Аквизиција дигиталних података

У овој фази подаци се изолују, обезбеђују и чувају. Да би се извршила даља аквизиција података неопходно је очувати интегритет података и обезбедити форензичку исправност података. То укључује спречавање људи да користе дигитални уређај како се дигитални докази не би мењали, као и формирање форензичке копије. Верификација дигиталног доказа се врши употребом хеша и то, MD5 или SHA1 [2].

Дигитални докази се могу разликовати по облику и врсти. Документи на рачунару, телефонска контакт-листа, спискови свих обављених телефонских позива, траг јачине сигнала са базне станице мобилног телефон, снимљене гласовне и видео-датотеке, разговори путем е-поште, обрасци мрежног саобраћаја, упади и откривање вируса, све су то примери различитих типова дигиталних доказа. Дигитални докази пре свега обухватају корисничке податке и метаподатке повезане са корисничким подацима, али и дневнике активности [2].

Кориснички подаци се односе на податке директно креиране или модификоване или којима приступа један или више корисника укључених у истрагу. Метаподаци, са друге стране, односе се на податке који пружају контекст о томе како, када, ко и у ком облику је креирао или модификовао податке корисника или истима приступио. Дневник активности представља запис о активностима корисника [2].

Када се дигитални доказ прибави, увек је потребно направити копије и спровести све форензичке тестове на таквим копијама, како било каква активност не би оштетила сачуване податке у оквиру оригиналних извора. Дигитални доказ се затим испита коришћењем једног или више форензичких алата.

В. *Анализа дигиталних података*

Форензичка анализа се дефинише као примена научних метода и критичког мишљења за решавање основних питања у истрази: шта, ко, зашто, како, када и где [2].

У фази анализе, дигитални форензичари користе одређене, пре свега, форензичке алате, уз помоћ којих врше преглед и анализу дигиталних трагова и доносе се закључци на основу пронађених доказа. Понекад може бити потребно понављање фазе анлизе, нарочито при прикупљању додатних оперативних сазнања која могу бити значајна за разрешење злочина, а која је потребно поткрепити одговарајућим доказима.

Г. *Документација*

Након анализе прави се записник који укључује све видљиве податке и који се предочава на суду. Често представљање дигиталних доказа на суду може бити у пратњи вештака ради сведочења [2].

IV. Форензички алати

Форензички алати су унапред дефинисани софтвер или методе које су доступне за примену у области дигиталне форензике [8]. Форензички алати не само да документују и чувају доказе, већ обезбеђују опоравак података у случајевима када је извршилац покушао да избрише и сакрије присуство неких кључних информација. Такође, ови алати пружају и друге услуге као што су формирање слике, провера историје претраживача, детаље за пријаву и одјаву, информације о IP адреси и још много тога [9].

Сврха форензичких алата је дата у наставку:

- Провера информација о датуму/времену
- Опоравак датотека и директоријума - "Carving"
- Претраживање кључних речи
- Опоравак интернет колачићаЛоцирање избрисаних или старих партиција дигиталних уређаја [3].

Коришћење одговарајућих алата ће омогућити

 ISBN 978-86-7466-969-3

компарацију дигиталних доказа, њихово лакше прикупљање, превод и заштиту података, документацију и презентацију дигиталних података добијених из дигиталног извора и помоћи да се добију поуздани докази и кључне информације о самом злочину.

А. Форензички алати у дигиталној форензици рачунара

Рачунарски форензички алати се користе за прикупљање података из система или рачунара. Користе се за набавку регистара и других шифрованих података са рачунара. Док се форензички алати за меморију користе за прикупљање и анализу нестабилне меморије рачунара (RAM - Random Access Memory). Различите платформе на којима ови алати раде су Windows, UNIX, Linux, DOS, MAC [9].

Форензички алати могу бити софтверски или хадверски. Између осталих, форензички алати који су нашли примену у форензици рачунара су Forensic Toolkit (FTK), EnCase и Magnet Axiom.

FTK је један од најстаријих форензичких софтвера. Због графичког интерфејса и рада на Windows оперативним системима постао је веома популаран. FTK омогућава корисницима да истраже и направе форензичку копију коришћењем његовог додатка FTK Imager који је „open source“. Има једноставан кориснички интерфејс, брзо и лако претраживање, могућност обележавања, креирања индекса кључних речи, могућност анализе података са различитих извора, креирања речника шифара, креирања извештаја. Ипак, поприлично је скуп, нема могућност обављања више процеса истовремено, постоји лимит у количини фајлова [10].

EnCase је програмски алат намењен форензичкој истрази дигиталних доказа фирме Guidance Software. Користи се од стране многих водећих компанија и организација у области дигиталне форензике. Омогућава и олакшава дигиталним форензичарима процес истраге, аквизиције и анализе доказног материјала и спречава измену података преузетих са корумпираног рачунара. Прибавља податке са широког спектра уређаја, укључујући и мобилне уређаје. Основне карактеристике и предности EnCase форензичког алата је што представља неинвазивни алат за форензичке истраге, прилагођен је форензичким истраживањима на великим количинама података, опремљен подршком за FAT, FAT32, NTFS, Apple, Unix, Linux оперативне системе, верификован је, тј. извештаји генерисани овим алатом потврђени су и прихваћени од стране правосудних органа ЕУ и САД. За разлику од FTK има могућност да анализира многе машине истовремено. Ипак, ово је скуп алат и његов кориснички интерфејс није тако једноставан као код FTK или Magnet Axiom [11].

Magnet Axiom је наменски направљен за опоравак, обраду и анализу дигиталних доказа из различитих извора, без обзира да ли се користи Magnet Axiom или неки алат треће стране за прикупљање података. Уз помоћ Magnet Axiom алата могу се опоравити и анализирати дигитални подаци, као и формирати извештај за прикупљене дигиталне доказе, било да се ради о рачунару, мобилном уређају или подацима са Cloud окружења, све у једном фајлу случаја. Пружа могућност опоравка и анализе податке из многих шифрованих апликација као што су Snapchat и Wickr. Axiom такође може да унесе податке од других алата за анализу, укључујући Cellebrite, Oxygen, GrayKey и друге. Има једноставан кориснички интерфејс, брзо и лако претраживање, могућност обележавања, креирања базе података кључних речи, креирања извештаја. Ипак, као и претходни алати, поприлично је скуп.Do not use justified vertical alignment for the page layout, and apply “Top” alignment instead. Do not use page numbering.

Б. Форензички алати у дигиталној форензици мобилних уређаја

Неки од популарниц форензичких алата који су значајни и имају примену за процес аквизиције и за анализу дигиталних доказа укључују Cellebrite UFED, FTK, XRY, Oxygen Forensic Suite, EnCase. Они се разликују по способностима и ефикасности у стицању информација добијених из различитих дигиталних уређаја. Међутим, сви ови софтверски алати нуде сличне услуге и прате сличне технике анализе. Мобилни оперативни системи који се истражују помоћу ових алата су Android, iOS, Blackberry OS, Windows и други. Мобилни уређаји користе две врсте копирања података приликом извођења екстракције података: физичку и логичку аквизицију. Приликом логичке аквизиције обично није могуће повратити избрисане податке, већ само извршити копију података који се налазе на логичком диску. Насупрот томе, физичка аквизиција обавља „бит-по-бит“ копију целог физичког диска и пружа могућност опоравка избрисаних датотека и других важних информација [12].

Поред података који се могу извући из меморије мобилног телефона (контакти, календар и белешке; поруке: SMS, EMS, MMS и гласовне поруке; евиденције позива: аудио и видео позиви; е-пошта; интернет историја; посећене url адресе; самосталне датотеке; GPS; информације о уређају: IMEI број), неки од ових алата пружају могућност добијања података из SIM меморије (ICCID и IMSI број; информације о телефонском именику; информације о позивима и порукама: SMS и EMS; као и информације о локацији као што је GPS [12].

В. Форензики алати у дигиталној форензици мрежа и „Cloud“ окружења

Мрежна форензика је релативно нова дисциплина дигиталне форензике која за циљ има обезбеђење сигурности података мрежа. Форензички алати у дигиталној форензици мрежа се састоје од више монитора који се могу инсталирати на различитим местима на мрежи и користе се за надзор. Ови алати за праћење

 ISBN 978-86-7466-969-3

мреже интегришу податке са различитих монитора и обезбеђују комплетан и свеобухватан приказ активности мреже.

Мрежни форензички алати могу се разврстати у неколико група: сервер за управљање и контролу (управља операцијама мрежних форензичких алата, из овог сервера постављају се програмски агенти, аквизицијски параметри, добављају се слике, те све остале акције прикупљања и анализе), сервер за складиштење података (служи за чување свих података преузетих са мрежних извора) и агенти (прикупљају и податке које OS не види или до којих нема приступа, а размештени су по истраживаним системима или мрежама).

V. Изазови дигиталне форензике

- Проблем сложености
- Проблем разноликости
- Конзистентност и корелација;
- Проблем количине или капацитета података за анализу

Пре свега, дигитални докази се добијају у сировом бинарном облику који је сложен са погледа разумљивости добијених података. Међутим, како су данас у употреби многобројни форензички алати за тумачење сирових дигиталних доказа, сложеност дигиталних података више не представља изазов. Са друге стране, у последње време, количина података прикупљених током дигиталних истрага стално расте и постаје неефикасан модел анализе сваког бајта. Обим и хетерогеност дигиталних доказа захтевају примену методе смањења података груписањем података у веће подскупове или уклањањем познатих и ирелевантних података пре анализа. Раст капацитета уређаја за складиштење представља додатан проблем. Такође, проблем настаје и при присуству више оперативних система, формата датотека и уређаја, јер не постоји стандардан начин за испитивање и анализу свих врста дигиталних доказа — то је довело до проблема разноликости. Осим тога, при спровођењу дигиталних истрага често дигитални форензичари имају податке са више извора, те је неопходно да се испита доследност и корелација доказа откривених у овим изворима. Форензички алати који тренутно постоје дизајнирани су да пронађу дигиталне доказе, али не помажу у самој истрази и анализи тих података, стога се већина анализа спроводи ручно. Пошто различити извори захтевају различите форензичке алате, ово је резултирало проблемом разноликости [2].

VI. Дигитална форензика будућности

Да би се у потпуности предвидела будућност дигиталне форензике, а пре свега форензике сајбер-криминала потребан је мултидисциплинарни приступ.

Најочигледнија промена ће бити у типу, величини и брзини медија за складиштење, меморији и процесору. У наредних 5 година, стандардни рачунари ће имати 5TB складишног простора, док ће флеш дискови носити 250 GB података. Дакле, биће потребно сортирати знатно већа количина података него данас. Међутим, рачунари ће постати и до 7 или 8 пута бржи (не узимајући у обзир развој квантног рачунарства). Форензички алати ће напредовати, развијајући способност аутоматизације прикупљања података и прелиминарне обраде. То значи да ће мање обучени људи моћи да користе форензичке алате. Међутим, сами рачунари ће вероватно еволуирати до сложености на коју нисмо навикли, будући да ће моћи да разумеју људски говор и доносе рационалне одлуке. Стога ће будући дигитални форензичар морати да се додатно специјализује, како би се бавио софистицираним знањем потребним за руковање софтвером и хардвером [8].

VII. Закључак

У овом истраживачком раду поменули смо различите врсте форензичких алата који се могу користити за решавање дигиталних злочина. У неким случајевима, алати су засновани на софтверу, али понекад је потребан и хардвер за прибављање доказа. Такође, неки од софтвера су бесплатно доступни, а неки се плаћају. Алати који се плаћају имају више функција у поређењу са „open source“ алатима и веома су скупи. Ипак, како је све заступљенији сајбер-криминал неопходно је да дигитална форензичка буде у корак са развојом дигиталних технологија и да развој форензичких алата превазиђе тренутне изазове са којима се сусрећу дигитални форензичари, а који утичу пре свега на квалитет и ефикасност форензичке истраге.

Без обзира на постојеће алате, развој дигиталног доба и развој технологије захтевају све тежа истраживања у дигиталној форензици. Много тога у вези са сајбер-безбедности се променило откако је пандемија приморала многе организације да усвоје удаљене и хибридне моделе рада за своје запослене. Ново радно окружење драстично је променило динамику приступа мрежи, коришћења уређаја и протокола сајбер-безбедности, готово преко ноћи. Данас је рад на даљину постао део новог хибридног модела рада који наставља да се примењује за многе организације што захтева промене постојеће технологије. Ипак, дигиталну форензику у будућности ће пратити низ промена које подразумевају развој најсавременије дигиталне форензичке технологије. Следећа генерација дигиталне форензичке технологије и форензичких алата, садржаће вештачку интелигенцију, аутоматизацију и решења за тренутне изазове дигиталне форензике Cloud окружења, што ће омогућити истражитељима форензичке алате који су им потребни да елиминишу тренутне форензичке изазове.

Захвалница

Овај рад је подржан од стране Криминалистичко - полицијског универзитета у Београду, Департмана форензичког инжењерства.

 ISBN 978-86-7466-969-3

Литература

[1] T. B. Tajuddin & A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone",World Congress on Internet Security, 2015.

[2] S. Raghavan, "Digital forensic research: current state of the art", CSI Transactions on ICT, Vol. 1(1), pp. 91–114 (2012).

[3] S. Yadav, K. Ahmad, & J. Shekhar, "Analysis of Digital Forensic Tools and Investigation Process",Communications in Computer and Information Science, pp. 435–441 (2011).

[4] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis & E. K. Markakis, E. K. " A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues", IEEE Communications Surveys Tutorials, Vol. 22(2), pp. 1191-1221 (2020).

[5] J. Kävrestad, "Fundamentals of digital forensics: Theory, methods, and real-life applications", Springer International Publishing, 2020.

[6] D.Lillis, B. Becker, T. O'Sullivan & M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation", Proceedings of the 11th Annual ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, Florida, pp. 24-26, 2016.

[7] M. Sarfraz, Cybersecurity Threats with New Perspectives, IntechOpen, 1(1), 2021.

[8] Dhwaniket Ramesh Kamble, Nilakshi Jain, "Digital forensic tools: a comparative approach", International Journal of Advance Research In Science And Engineering, Vol. 4(2), February 2015.

[9] Mayur Patankar, Deepika Bhandari, "Forensic Tools used in Digital Crime Investigation Forensic Science", Forensic Science, Vol. 4(5),| pp.278-283, May 2014.

[10] Извор: https://www.exterro.com/forensic-toolkit, Приступљено: 01.05.2023. године.

[11] Д. Ранђеловић, Д. Делија, Б. Поповић , „EnCase форензички алат", Безбедност, Београд 51, 1-2, pp. 286-312 (2009).

[12] T. B. Tajuddin & A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone", World Congress on Internet Security (WorldCIS), 2015.

[13] R. Đokić, i dr., „Forenzika računarskih mreža", Vojnotehnički glasnik,, Vol. 53 (1), pp. 136–145 (2013).

 ISBN 978-86-7466-969-3