Зборник радова Факултета техничких наука, Нови Сад

UDK: 004.738.1:766
DOI: https://doi.org/10.24867/29BE11Miljkovic

ФОРЕНЗИКА macOS-а

MacOS FORENSICS

Душан Миљковић, Факултет техничких наука, Нови Сад

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Дигитална форензика представља важну област информатике, а један од најважнијих аспеката дигиталне форензике односи се на оперативне системе који представљају срце сваког рачунарског уређаја. У овом раду обрађена је тема дигиталне форензике macOS-а кроз анализу самог оперативног система, као и метода и алата за форензику оперативног система macOS. На крају је одрађена и студија случаја која приказује како се неке од метода и алата могу користити за дигиталну форензику.*

Кључне речи: *дигитална форензика, macOS*

Abstract – *Digital forensics represents an important field of computer science, and one of the most crucial aspects of digital forensics relates to operating systems, which form the heart of every computing device. This paper addresses the topic of macOS digital forensics by analyzing the operating system itself, as well as the methods and tools for macOS forensics. Finally, a case study is presented, demonstrating how some of these methods and tools can be used for digital forensics.*

Keywords: *digital forensics, macOS*

1. УВОД

Дигитална форензика представља важну област информатике која се бави проналажењем, анализом и интерпретацијом дигиталних података како би се расветлили различити облици кривичних дела и инцидената. У савременом друштву, где се дигитални уређаји и мреже налазе на сваком кораку и њихов број је све већи и већи, дигитална форензика игра неизоставну улогу у процесу разоткривања кривичних дела и осигуравању доказа неопходних за судске поступке.

У овом раду обрађена је тема дигиталне форензике MacOS-а. MacOS се истиче високим стандардима сигурности и безбедности, са нагласком на заштиту корисничких података и интегритета система.

Први део овог рада детаљније објашњава шта је дигитална форензика који су то принципи дигиталне форензике, процеси и области.

Након тога, описан је macOS, његова историја, архитектура, фајл систем и безбедносни механизми.

Затим следи поглавље о техникама за форензику macOS-а, са освртом на битне артифакте, њихово прикупљање и анализу. После тога следи и поглавље о алатима за форензику macOS-а.

За сам крај одрађена је студија случаја која приказује како се неке од претходно поменутих метода и алата могу користити у дигиталној форензици.

2. ДИГИТАЛНА ФОРЕНЗИКА

Дигитална форензика, која се понекад назива и компјутерска форензика, представља научну дисциплину чији предмет су идентификација, прикупљање, чување, прегледање, анализа и презентација дигиталних доказа коришћењем научно и правно ваљаних метода и алата [1].

2.1. Историја дигиталне форензике

Успон дигиталне форензике је започео осамдесетих година, када је FBI покренуо први званични програм за магнетне медије, а значајни напредак је постигнут током деведесетих и двехиљадитих због потребе за борбом против дечије порнографије и анализе дигиталних уређаја у војним операцијама. Прекретница у професионализацији дигиталне форензике догодила се 2006. године са увођењем обавезног режима за електронско откривање у Правилима о парничном поступку САД [2].

2.2. Примена дигиталне форензике

Дигитална форензика постала је изузетно значајна због савременог развоја информационих и комуникационих технологија које су довеле до пораста дигиталног криминала и до пораста безбедносних инцидената.

Примена дигиталне форензике је веома велика, од решавања сајбер криминала, преко правосуђа па све до рекламација и различитих спорова [1].

2.3. Области дигиталне форензике

Дигитална форензика дели се на неколико грана (подобласти), у зависности од уређаја, система који преноси дигиталне доказе или од самог дигиталног доказа. Тако постоји дигитална форензика рачунара, форензика рачунарских мрежа, форензика мобилних уређаја, форензика мултимедијалних записа итд, али с обзиром на то да се информационе технологије јако брзо мењају, релативно брзо настају и нове области

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

дигиталне форензике као што су дигитална форензика уграђених система (енг. embedded systems), форензика IoT, форензика облака (енг. cloud) итд. [1].

2.4. Принципи дигиталне форензике

Како би се осигурала тачност, ефикасност и прихватљивост доказа, дигитални форензичар мора испоштовати основне принципе који се примењују у свим областима дигиталне форензике, а то су: користити научно прихваћене методе и алате, стриктно пратити протоколе, обезбедити ланац доказа, документовати процес и не мењати ништа на изворном медијуму [1].

2.5. Нивои апстракције

Докази се могу посматрати на различитим нивоима апстракције, за шта се користе различите технике и алати. Рад на најнижем нивоу апстракције је пожељан јер пружа највише информација, али може захтевати више времена, па се понекад праве изузеци када је потребна брза анализа [3].

2.6. Нивои волатилности (несталности) доказа

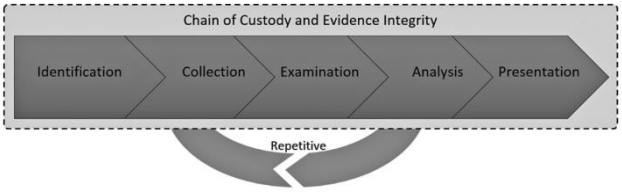
Волатилни (нестални) подаци односе се на информације смештене у привременој меморији система, као што је RAM или физичка меморија, и у активним процесима или сервисима. Ови подаци се карактеришу њиховом привременом природом; постоје само док је систем укључен и могу бити изгубљени или измењени при гашењу или поновном покретању система [1].

2.7. Процеси дигиталне форензике

Дигитални докази могу се наћи на различитим дигиталним уређајима и системима. Примена форензичког процеса осигурава исправност истраге кроз два основна принципа:

- **интегритет доказа**, који подразумева очување доказа у његовом изворном облику, и
- **ланац доказа**, који захтева документовање свих акција учињених на доказима како би се доказала њихова аутентичност и интегритет.

Цео истражни процес може се поделити у пет итеративних фаза: идентификација, прикупљање, прегледање, анализа и презентација доказа [1].



Слика 1. *Процеси дигиталне форензике [1]*

2.8. Дигитална форензика оперативних система

Форензика оперативног система представља процес прикупљања корисних информација из оперативног система рачунара или мобилног уређаја са циљем стицања емпиријских доказа против починиоца. Испитивање конфигурационих фајлова може помоћи у утврђивању догађаја на рачунару, за шта је потребно разумевање оперативног система и његовог фајл система [4].

3. MacOS

Почеци MacOS-а датирају још од 1984. године, када је Apple представио Macintosh, први комерцијални рачунар са графичким корисничким интерфејсом и мишем. Ово је значајно олакшало коришћење машина и учинило их доступнијима за људе који нису толико заинтересовани за технологију. Apple је ову верзију назвао системски софтвер, или једноставно систем [5].

3.1. Класични MacOS

Софтвер се састојао од два фајла видљива корисницима: системског фајла и Finder-а који су се налазили у фолдеру са ознаком „системски фолдер“ (енг. system folder). Како ране верзије MacOS-а нису имале специфична имена, људи су почели да користе верзије системских фајлова како би разликовали различите верзије оперативног система, па је првобитна верзија позната и као систем 1. Прве верзије MacOS-а познате су и под називом „класични” MacOS, а објављено је девет главних верзија класичног MacOS-а [6].

3.2. MacOS X

MacOS X, заснован на Unix архитектури, представља наследника класичног MacOS-а и представљен је 2001. године. Овај оперативни систем донео је велику стабилност, сигурност и нове функције у свет Macintosh рачунара. Са својим Aqua интерфејсом, систем је понудио естетски привлачан и интуитиван кориснички доживљај. Међу значајним карактеристикама су Spotlight за претрагу, Time Machine за бекап, и интеграција са iCloud-ом за синхронизацију података. Од 2012. године назив оперативног система је промењен у OS X, а од 2016. године, како би ускладио брендирање са брендирањем других примарних оперативних система компаније, Apple мења назив оперативног система у macOS [6].

3.3. MacOS (од 2020. године)

Од 2020. године, Apple је започео нову еру за MacBook рачунаре, увећавајући главну верзију оперативног система са 10 на 11 и доневши први редизајн корисничког интерфејса након 6 година. Велика измена је била прелазак на Apple Silicon чипове, што је донело знатна убрзања у раду и ефикасности система.

3.4. Архитектура macOS-а

MacOS направљен је за Macintosh рачунаре и изграђен је на основама базираним на UNIX-у. Архитектура оперативног система укључује неколико кључних компоненти.

Језгро macOS-а чини **XNU** кернел, он представља хибридни кернел чија су три основна дела Mach кернел развијен на Карнеги Мелон универзитету (енг. Carnegie Mellon University), BSD и C++ API за писање драјвера назван I/O-Kit.

APFS представља основни фајл систем за све оперативне системе унутар Apple-а, macOS-а, iOS, watchOS и tvOS. Од 2017. године он замењује HFS+ као

основни фајл систем, док је коначна верзија APFS-а објављена 2018. године. Неке од најзначајнијих његових карактеристика:

- Наносекундска временска ознака
- Дељење простора
- Скоро тренутно копирање података
- Snapshots (read-only инстанце фајл система на волумену)
- Шифровање

Многи артифакти од интереса на macOS систему чувају се као property list или .plist фајлови. Постоје два типа property list-ова: обични текстуални, тј. XML plist и бинарни plist фајлови. Обични текстуални plist фајлови могу се директно прегледати или видети у било ком програму за приказ XML-а, док се бинарни морају претворити у обични текст пре анализе. Због тога што су компактнији од својих еквивалената бинарни property list фајлови постају све чешће коришћени [7].

3.5. Безбедносни механизми

Apple дизајнира безбедност у сржи својих платформи. Сваки Apple уређај комбинује хардвер, софтвер и сервисе дизајниране да раде заједно како би постигли максималну безбедност и транспарентно корисничко искуство са циљем да личне информације остану сигурне.

Са првим издањем Apple Silicon чипа, значајно је унапређена безбедност и приватност корисника, уводећи функционалности као што су безбедно покретање, AES хардверски механизам за шифровање и Secure Enclave. Ови чипови осигуравају безбедно покретање уређаја од Boot ROM нивоа и имају Secure Enclave који штити осетљиве корисничке податке, укључујући и биометријске информације.

Механизам ажурирања софтвера и системска заштита интегритета (SIP) додатно доприносе повећању безбедности, спречавајући неовлашћени приступ и манипулацију системским компонентама, што додатно штити корисничке податке и оперативни систем [7].

4. ТЕХНИКЕ ЗА ФОРЕНЗИКУ MAC OS-A

Технике дигиталне форензике помажу да се провери неалоцирани простор на диску као и скривени фолдери за копије шифрованих, оштећених или обрисаних фајлова. Неке од најчешћих техника за форензику су: imaging, live forensics, претрага по кључним речима, враћање података, стегоанализа, анализа временске линије и друге [8].

4.1. Imaging

Приликом прављења дигиталне копије оригиналног диска (енг. imaging) macOS-а, најпре је потребно утврдити о ком моделу рачунара се ради. Уколико се ради о новијим верзијама система које користе Apple M серију чипова, неопходно је познавање корисничке шифре јер у супротном није могуће приступити подацима [8].

4.2. Анализа Apple метаподатака

У домену дигиталне форензике, метаподаци играју кључну улогу у откривању информација о фајловима, фолдерима и активностима које их окружују. Метаподаци, у суштини подаци о подацима, пружају драгоцене увиде у атрибуте фајлова, временске ознаке, порекло и интеракције корисника. У оквиру macOS екосистема, Apple метаподаци нуде богат извор форензичких доказа, а команда mdls служи као моћан алат за издвајање и анализу ових метаподатака [9].

4.3. Анализа .plist фајлова

Анализа .plist фајлова у дигиталној форензици пружа драгоцене увиде у активности корисника, обрасце коришћења апликација, конфигурације система и потенцијално злонамерне активности. Форензички истражитељи екстрахују и анализирају .plist фајлове помоћу различитих алата, откривајући кориснички подешавања, мрежна повезивања и конфигурације апликација. Метаподаци и временске ознаке у .plist фајловима помажу у успостављању временских линија активности корисника и системских догађаја. Форензичка анализа ових фајлова може наићи на изазове као што су рад са бинарним фајловима и идентификација релевантних података међу многобројним .plist фајловима [10].

4.4. Остали артифакти значајни за дигиталну форензику

Поред .plist фајлова, Apple има мноштво других артифаката који могу помоћи у бољем разумевању тока података. Knowledge C база података складишти разне типове података о интеракцијама и активностима корисника. Bash/Zsh историја садржи командну историју и информације о сесијама. FSEvents у корену партиције садржи логове и информације о фајл системским догађајима. QuarantinedEventsV2 база података прати и управља информацијама о фајловима преузетим са интернета и стављеним у карантин.

5. АЛАТИ ЗА ФОРЕНЗИКУ MAC OS-a

За дигиталну форензику је кључно да алати производе поуздане доказе који испуњавају стандарде прихватљивости на суду, захтевајући поновљивост и репродуктивност резултата тестова. Форензички алати морају бити тестирани по NIST стандардима и прихваћени на суду како би резултати били валидни. Постоји велики број комерцијалних и алата отвореног кода који се користе у дигиталној форензици [8].

5.1. Комерцијални алати

Apple редовно ажурира свој оперативни систем, унапређујући безбедност, што форензичарима отежава прикупљање података са MacBook рачунара и захтева стално ажурирање алата. Комерцијални форензички алати нуде могућности као што су блокирање уписивања, клонирање дискова, опоравак скривених и обрисаних фајлова, удаљено и live прикупљање доказа, анализа RAM-а, напредно претраживање и филтрирање података и метаподатака, као и аутоматско генерисање извештаја. Најпознатији алати укључују EnCase, BlackBag MacQuisition, Magnet AXIOM, Sumuri Recon LAB и Sumuri Recon ITR.

5.2. Алати отвореног кода

Коришћење алата отвореног кода у дигиталној форензици нуди бројне предности, укључујући бесплатно индивидуално образовање форензичара. Ови алати су преносиви и флексибилни, омогућавајући коришћење на различитим системима и на више начина, и могу потврдити налазе комерцијалног софтвера. Највећа предност је приступ њиховом коду, који се може уређивати и прилагођавати специфичним потребама корисника. Два најпознатија алата отвореног кода која се користе за форензику macOS-а су The Sleuth Kit и Autopsy.

6. СТУДИЈА СЛУЧАЈА

Анализа дигиталних уређаја постала је кључна компонента у истрагама савремених кривичних дела, посебно када је у питању злоупотреба истих. Студија случаја фокусира се на форензичку истрагу macOS-а у контексту злочина продаје података о кредитним картицама. Студија се спроводи са циљем да се открије да ли и у којој мери је могуће идентификовати, сакупити и анализирати релевантне дигиталне доказе који би потврдили незаконите активности извршене на MacBook рачунару. Методе које су се користиле у истрази јесу imaging и претрага по кључним речима, а од алата је коришћен Sumuri-ев Recon ITR.

Анализирани су подаци са лаптопа који је коришћен за почињење кривичног дела продаје података о кредитним картицама.

Најпре, извршена је претрага по кључним речима којом се идентификовао извор комуникације, а затим детаљном анализом утврђено је да је починилац користећи GnuPG библиотеку извршио криптовање података, и тако криптоване послао назад кориснику. Такође, на основу порука, утврђена је и договорена цена за коју је починилац починио кривично дело, а да је тек након уплате новца и потврде трансакције послао енкриптоване податке. Анализа ових доказа омогућила је да се утврди тачно време и датум када су спорне активности извршене, као и да се идентификују корисници који су исте починили.

7. ЗАКЉУЧАК

Дигитална форензика представља неизоставан део савремених истрага кривичних дела, посебно у ери у којој су дигитални уређаји и мреже свеприсутни. Људи користе паметне уређаје на сваком кораку, непрестано остављајући дигиталне трагове, а веома често су и несвесни њиховог постојања. Сваки клик, претрага или комуникација оставља дигитални отисак који се може искористити у форензичкој истрази.

Овај рад пружио је свеобухватан преглед принципа и процеса дигиталне форензике, са посебним фокусом на оперативни систем macOS. Размотрени су његови безбедносни механизми, важни артифакти, методе, технике и алати који се користе за форензичке анализе.

Студија случаја показала је да је уз познавање корисничке шифре могуће извршити тријажу новије серије MacBook лаптопова и креирати форензичку слику.

8. ЛИТЕРАТУРА

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

[2] https://raf.edu.rs/citaliste/clanci/svastara/sta-je-to-digitalna-forenzika-i-kako-naci-posao-u-tom-mocnom-polju/ (приступљено у августу 2023)

[3] https://citeseerx.ist.psu.edu (приступљено у августу 2023)

[4] https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9678340 (приступљено у априлу 2024)

[5] https://www.macworld.com/article/793119/macos-history-video-system-0-97-to-macos-13-ventura.html (приступљено у марту 2024)

[6] https://www.youtube.com/watch?v=_K5e8dJtMgE (приступљено у марту 2024)

[7] https://developer.apple.com (приступљено у марту 2024)

[8] Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar - Cybercrime and Digital Forensics, Routledge 2022

[9] https://www.youtube.com/watch?v=gcalmiLpZcc (приступљено у априлу 2024)

[10] https://www.magnetforensics.com/resources/macos-forensic-artifacts-and-techniques-apr8/ (приступљено у априлу 2024)

Кратка биографија:

Душан Миљковић је рођен у Лесковцу 1995. године. Основне академске студије завршио је на Војној академији у Београду, смер „Војноелектронско инжињерство“, а мастер студије на Факултету техничких наука у Новом Саду, смер „Софтверско инжењерство и информационе технологије“

Контакт: dusanmiljkovic_95@hotmail.com