Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.738.1:766
DOI: https://doi.org/10.24867/16BE25Radic

ФОРЕНЗИКА СКЛАДИШТА У ОБЛАКУ

CLOUD STORAGE FORENSICS

Дијана Радић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИЧКО И РАЧУНАРСКО ИНЖЕЊЕРСТВО

Кратак садржај – *У раду су анализиране технике и алати форензике складишта у облаку. Главни фокус рада је на изазовима на које се наилази приликом бављења форензиком облака. Дат је осврт на оквир дигиталне форензике облака, на технике и процесе који се предузимају приликом истраге и на софтверске и хардверске алате који се користе. Такође, споменути су неки од правних аспеката форензике облака са којима треба бити упознат. У оквиру рада илустрована је и студија случаја која има за циљ да читав процес заокружи и симулира на хипотетичком примеру.*

Кључне речи: *форензика складишта у облаку, рачунарство у облаку, дигитална форензика, технике, алати, докази*

Abstract – *In this paper, cloud storage forensics technique and tools are analyzed. The main focus of the paper is on the challenges encountered when dealing with cloud forensics, digital cloud forensics framework, techniques and processes undertaken during the investigation, and the software and hardware tools used. Some of the legal aspects of cloud forensics, that forensics investigators need to be familiar with, are also mentioned. The paper also illustrates a case study that aims to complete and simulate the whole process on a hypothetical example.*

Keywords: *cloud storage forensics, cloud computing, digital forensics, techniques, tools, evidence*

1. УВОД

Складиште у облаку дизајнирано је за пословне или личне сврхе и омогућава корисницима разне услуге. Већина људи већ користи разне услуге рачунарства у облаку, а да тога нису ни свесни. Gmail, Google Drive па чак и Facebook и Instagram су апликације засноване на облаку.

Приступ облаку могућ је и преко телефона и преко рачунара. Један од главних аспеката форензичког истраживања складишта у облаку је открити шта је корисник урадио од тренутка претплате на услугу до краја коришћења услуге.

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

Овај рад обрађује форензику облака. У другом одељку обрађено је рачунарство у облаку. Трећи одељак се бави дигиталном форензиком. Четврти одељак образлаже технике специфичне за форензику складишта у облаку, као и изазове са којима се дате технике суочавају. Кроз пети одељак уводе се хардверски и софтверски алати који се користе током истрага везаних за дигиталну форензику складишта у облаку. Једна од незаобилазних ставки сваког истражитеља који се бави форензиком облака јесте правни аспект ове теме који је обрађен у шестом одељку. Седми одељак доноси студију случаја на хипотетичком примеру како би се илустровао процес форензичке истраге у облаку који је обрађен кроз претходна поглавља. У осмом одељку дата су завршна разматрања.

2. РАЧУНАРСТВО У ОБЛАКУ

Амерички Национални институт за стандарде и технологију (NIST) је 2011. године објавио дефиницију која је често цитирана: „Рачунарски облак је модел који омогућава свуда присутан, погодан мрежни приступ дељивим рачунарским ресурсима (рачунарским мрежама, серверима, складишту података, апликацијама и сервисима), који на захтев корисника и уз минималну интеракцију са испоручиоцем услуга, могу бити брзо стављени на располагање кориснику или отказани".

Карактеристике облака су:

- Пружање услуге на захтев корисника
- Широк мрежни приступ
- Удруживање ресурса
- Брза еластичност
- Измерена услуга

Услуге у облаку су генерално категорисане у три модела услуге: (1) инфраструктура као услуга (IaaS - infrastructure as a service), (2) платформа као услуга (PaaS - platform as a service) и (3) софтвер као услуга (SaaS - software as a service); и четири модела примене: (1) јавни, (2) приватни, (3) хибридни и (4) заједнички. Количина контроле, одговорност и видљивост коју корисник има над оперативним системом, апликацијама и системским софтвером као што су веб сервер и системи за управљање базама података јесте фактор за разумевање разлика између модела.

2.1 Виртуализација

Виртуализација представља један од темеља на којем је изграђено рачунарство у облаку и без којег не би постојало. Виртуализација је технологија која

омогућава креирање ИТ услуга користећи ресурсе који су традиционално везани за хардвер. Омогућава коришћење пуног капацитет физичке машине дистрибуирањем њених могућности међу многим корисницима или окружењима [1].

2.1 Вишеклијентски систем

Вишеклијентски систем сугерише да један ресурс, у случају рачунарства у облаку један сервер, деле потенцијално више корисника. Количина корисника који деле одређене услуге у облаку разликује се по моделима услуге и примене. На пример, у IaaS моделу хардвер ће се делити на више закупаца али оперативни системи и системски софтвер неће. У PaaS-у оперативни систем и системски софтвер могу да се деле са другим корисницима, али апликације се не деле [2]. На крају у SaaS-у се може десити да се чак и иста инстанца физичке базе података дели са другим корисницима.

3. ДИГИТАЛНА ФОРЕНЗИКА

Дигитална форензика је научна дисциплина чији предмет су идентификација, прикупљање, чување, прегледање, анализа и презентација дигиталних доказа коришћењем научно и правно ваљаних метода и алата. Најважнији циљ форензичке истраге је да доведе у корелацију чињенице, особе и друге ентитете извучене са дигиталног уређаја [3].

Два принципа доминантна за дигиталну форензику јесу интегритет доказа и обезбеђивање ланца надлежности.

3.1. Процес дигиталне форензике

Постоји пет узастопних, али и итеративних фаза у процесу дигиталне форензике. Укратко, прва фаза је идентификација уређаја који би потенцијално могли да садрже доказе релевантне за истрагу. У другој фази се са идентификованих уређаја прикупљају докази. Трећа фаза јесте припрема сирових доказа како би се касније лакше обрадили и анализирали. Четврта фаза јесте коначно анализа где се покушавају разумети докази и утврдити след догађаја. Последња фаза је презентовање налаза суду или субјекту од интереса.

3.2. Форензика складишта у облаку

Форензика складишта у облаку представља подграну форензике мреже. Према дефиницији NIST-а 2014: „Форензика рачунарства у облаку је примена научних принципа, технолошке праксе, изведених и проверених методе за обраду прошлих догађаја у облаку идентификацијом, прикупљањем, чувањем, прегледом и извештавањем о дигиталним подацима у сврху олакшавања реконструкције ових догађаја“.

Форензика складишта у облаку има три димензије:

- Техничка димензија
- Правна димензија
- Организациона димензија

Техничка димензија: Ову димензију одликује употреба алата за извођење форензике рачунарства у облаку. Прикупљање података, форензика уживо, праћење комуникације преко мреже и декрипција су неки од задатака који се решавају. Алати се међусобно разликују у погледу њиховог развојног модела и услужног модела.

Правна димензија: Споразум о нивоу услуге (SLA - Service Level Agreement) је медиј за осигурање сигурности података између провајдера услуге у облаку и потрошача. Како би се гарантовала приватност, форензички поступак не би требало да крши ниједан закон и пропис у надлежности центра за обраду података.

Организациона димензија: Провајдер и клијент су главни актери форензичке истраге у облаку међутим постоји и трећа страна тј. три врсте трећих страна које су укључене у истражни процес:

- ИТ стручњаци
- Руковаоци инцидентима
- Правни саветници [4].

Две фазе дигиталне форензике које су највећи изазов за форензику облака јесу идентификација и прикупљање.

4. ТЕХНИКЕ У ФОРЕНЗИЦИ ОБЛАКА

4.1. Анализа лог записа из складишта у облаку

Лог је порука коју рачунарски систем, уређај или софтвер генерише као одговор на неки стимуланс. Стимуланс може да буде акција корисника, грешка у раду апликације или нека друга активност. Типична лог порука се састоји из временске одреднице, извора и података. Логови могу да имају више извора настанка међу њима оперативне системе, рутере, свичеве, бежичне приступне тачке, firewall (заштитни зид), VPN сервере, штампаче итд. Постоји више врста лог фајлова у зависности од тога где су настали и која им је намена.

Због повећане употребе интернета и иновација у технологијама облака, повећао се број рањивости и напада у облаку. Сви ови напади могу да се прате кроз логовање [5].

4.2. Прикупљање доказа кроз веб претраживач

Веб претраживач може бити кључан за дигиталну истрагу, складишти податке о употреби интернета као и неке себи својствене податке у зависности од врсте претраживача. Неки од артефаката који се прикупљају су историја прегледања, кеш, сесије, колачићи, итд.

Према последњим истраживањима највише се користи Chrome са преко 60% удела, након њега иде Safari са око 18%. Када се утврди која врста претраживача коришћена на идентификованим уређајима, артефакти се траже на локацијама на којима их претраживачи складиште.

4.3. Праћење мрежног саобраћаја

Приступ облаку је немогућ без интернета, зато је и праћење мрежног саобраћаја значајно ако за то постоји могућност.

Користећи разне алате могуће је ухватити информације које се преносе и користити њих даље кроз истрагу. Мрежна форензика је често везана за праћење и анализу нестабилног и динамичког саобраћаја на мрежи.

Форензичар тражи податке који могу бити у једном од три облика: статичном, покретном или унутар процеса који се извршава. Мрежна форензика се односи на приступ који укључује употребу наменске инфраструктуре која може прикупљати, очувати и анализирати мрежни саобраћај у сврху истраге [6].

4.4. Изазови техника форензичке истраге облака

Неки од изазова у техникама за форензику облака по фазама форензичке истраге:

Идентификација:

- Није позната физичка локација података,
- Питање јурисдикције,
- Зависност од провајдера услуге у облаку
- Може да се догоди да сви подаци нису на једном месту, због децентрализованости података.
- Сегрегација доказа, како прикупити само релевантним подацима са сервера који опслужује више клијената

Прикупљање:

- Недоступност података
- Вишеклијентски систем
- Обрисани подаци

Анализа:

- Енкрипција података
- Непостојање јединственог шаблона за лог фајлове

5. АЛАТИ У ФОРЕНЗИЦИ ОБЛАКА

Алати који се развијају специјално за дигиталну форензику морају да гарантују прецизност и поузданост.

5.1. Мобилни теренски комплет – Mobile Field Kit

Унутар комплета се налази лиценцирани софтвер уграђен на Windows систему, каблови, прикључци за пуњење, камера за снимање телефона, једна средња и једна већа Фарадејева врећа за телефоне и таблете, све је то спаковано у ојачани кофер за пренос.

Како се докази везани за форензику облака често налазе у центрима података и није могуће испитивања извршити у лабораторији, мобилни теренски комплет је неопходан за прикупљање доказа и њихову заштиту.

5.2. UFED Cloud Analyzer

UFED Cloud Analyzer је производ компаније Cellebrite. Овај алат може да се користи за прикупљање, очување и анализу доказа са облака. Подаци могу да се сортирају, филтрирају, претражују и да се аутоматски генеришу извештаји.

Има следеће карактеристике:

• Прибавља историју прегледа и претраге и сортира у хронолошком реду.

• Прикупља податке са најпопуларнијих друштвених мрежа и складишта у облаку, уз помоћ креденцијала корисника или токена прикупљеног са уређаја.

5.3. FTK Imager

FTK Imager је бесплатан софтверски алат, развијен од стране компаније AccessData. Главна функција овог алата је да направи копије компјутерских података без њихове промене. Има следеће карактеристике:

• Могућност креирања форензичких слика са хард дискова, CD-ова, DVD-ова, целог фолдера или појединачног фајла итд.

• Може да поврати фајлове који су обрисани из корпе за смеће, уколико подаци нису преписани неким новим подацима.

• Може да израчуна хеш вредност креираних форензичких слика користећи једну од две доступне опције Message Digest 5 (MD5) и Secure Hash Algorithm (SHA-1).

5.4. Wireshark

Wireshark је алат отвореног кода који се употребљава за тестирање мреже, решавање проблема и проверу различитог саобраћаја који пролази кроз рачунарску мрежу анализом мрежних пакета.

Сва комуникација и размена података корисника, преко свог налога, са услугама складиштења у облаку се одвија и преноси путем интернета. Потенцијалним анализирањем података прикупљених са мреже могуће је доћи до доказа релевантних за ток истраге.

6. ПРАВНИ АСПЕКТИ У ФОРЕНЗИЦИ ОБЛАКА

6.1. Територијалност података – губитак локације

Већина провајдера услуга складишта у облаку има неколико центара података расутих по целом свету ради редундантности података и оптимизације перформанси.

Приликом сваког отпремања датотеке у облак, она се аутоматски множи и складишти у најмање две (обично три) засебне географске и физичке локације, обично у различитим земљама.

Правна теорија наводи да је законодавство које се треба применити одређено местом на коме се одиграо кривични догађај. Други територијални приступ скреће пажњу на медиј са којим је злочин извршен. Локација крајњег корисника је трећи приступ изазова територијалности података.

Држављанство починиоца или жртве се користи као одлучујући критеријум у четвртом територијалном приступу, без обзира на локацију на којој је злочин извршен [7].

Како би се примена овог принципа регулисала на међународном нивоу, суверене државе међусобно склапају уговоре.

6.2. Власништво над садржајем облака

Провајдер услуга у облаку не поседује ни један податак са правне тачке гледишта.

Да би се неко могао сматрати кривично одговорним за „поседовање“ одређене датотеке, услов који мора да испуни јесте да ју је барем једном „прегледао“ [7].

Може се тврдити да би се облак требао сматрати и правно третирати као виртуелни и удаљени екстерни медиј за складиштење (тј. заправо да је то продужетак сваког дигиталног уређаја који му има приступ). Кључни елемент на основу којег је основана кривична одговорност је намерно и свесно приступање упитним датотекама личним чином [7].

6.3. Очување података

Чланови 16. и 29. Будимпештанске конвенције о сајбер криминалу [8] наводе да су земље потписнице дужне да предузму законодавне мере у вези са потенцијално убрзаним очувањем одређених ускладиштених рачунарских података који су ускладиштени помоћу рачунарских система који се налазе на њиховој територији, посебно тамо где постоје основане сумње да су рачунарски подаци посебно рањиви на губитак или измену. Међу земљама потписницама се налази и Србија.

7. СТУДИЈА СЛУЧАЈА

7.1. Припрема

Претпоставка је да је полиција добила дојаву о инциденту који укључује складиште у облаку. Потребно је утврдити где је провајдер облака регистрован, како би се утврдило да ли поседују јурисдикцију да обаве истрагу.

7.2. Идентификација

Како су данас мобилни телефони и рачунари у широкој употреби, претпоставка је да су ови уређаји заплењени приликом претреса. Пронађени уређаји се фотографишу на месту проналаска и праве се забелешке о њима укључујући забелешке о моделу, марки, серијском броју уређаја итд.

7.3. Прикупљање

Ако је којим случајем рачунар био укључен, потребно је прикупити несталну меморију. Ово може да се обави користећи FTK Imager. Неопходно је да истражитељ пажљиво изврши прикупљање несталне меморије јер ће након гашења уређаја она нестати. Са истим алатом може да се направи форензичка слика хард диска.

За прикупљање података из складишта у облаку постоји више сценарија у зависности од јурисдикције. Провајдер услуге може на захтев истражитеља да прикупи податке, пратећи савете које добије и користећи правно ваљане технике и алате, ако истражитељ то не може лично да уради. Ово је сценарио уколико истражитељи имају надлежност.

7.4. Прегледање

У фази прегледања сви прикупљени уређаји и креиране копије се преносе у лабораторију. Приликом прегледања истражитељ мора да покуша да дешифрује криптоване податке и да поврати податке који су обрисани.

7.5. Анализа

Када заврши припрему доказа прелази се на анализирање и извлачење закључака.

7.6. Презентација

На крају се креира извештај који описује процес и проналаске истраге. Одабрани релевантни пронађени фајлови се могу доставити копирани на CD-у.

8. ЗАКЉУЧАК

Област форензике складишта у облаку је у константном развоју јер постоје проблеми који још нису решени. Такође, са напретком технологије појављиваће се и нови проблеми и изазови који ће захтевати посебну пажњу.

Сваки случај или инцидент јесте јединствен. Оквир истраге може бити исти, али алати и технике се морају прилагодити случају. Мора се водити рачуна да примењени алати и технике морају имати кредибилитет на суду и да су довољно испитани да се може гарантовати интегритет доказа који се помоћу њих обрађују.

9. ЛИТЕРАТУРА

[1] Red Hat, Inc., What is virtualization?, Red Hat, June 2018. [Online]. Доступно: https://www.redhat.com/en/topics/virtualization/what-is-virtualization (приступљено у септембру 2021.)

[2] Greg Gogolin, PhD, CISSP, Digital Forensics Explained, 2nd ed. Boca Raton, Taylor & Francis Group, LLC, 2021

[3] Flora Amato, Aniello Castiglione, Giovanni Cozzolino, Fabio Narducci, A semantic-based methodology for digital forensics analysis, Journal of Parallel and Distributed Computing vol. 138 , pp. 172–177, Jan. 2020

[4] A. M. Poorvi Jain, "Review of Cloud Forensics: Challenges, Solutions and Comparative Analysis,"International Journal of Computer Applications, pp. 28-34, 2019.

[5] Thankaraja Raja Sree and Somasundaram Mary Saira Bhanu, "Data Collection Techniques for Forensic Investigation in Cloud", Intechopen Digital Forensic Science, Sep 2020, [online] Available: http://www.grandviewresearch.com.

[6] N. Raza, "Challenges to network forensics in cloud computing," 2015 Conference on Information Assurance and Cyber Security (CIACS), 2015, pp. 22-29, doi: 10.1109/CIACS.2015.7395562.

[7] Karagiannis, C.; Vergidis, K. Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. Information 2021, 12, 181. https://doi.org/10.3390/info12050181

[8] Council of Europe. Convention on Cybercrime. [Online]. Доступно: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (приступљено у септембру 2021.)

Кратка биографија:

Дијана Радић рођена је у Сомбору 1997. године. Завршила је основну школу „Никола Тесла“ у Бачком Брестовцу, затим гимназију „Вељко Петровић“ у Сомбору. Дипломирала је 2020. на Факултету техничких наука у Новом Саду, смер Рачунарство и аутоматика.