Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.42:004.738.12
DOI: https://doi.org/10.24867/18BE27Sekulic

ФОРЕНЗИКА ОПЕРАТИВНОГ СИСТЕМА WINDOWS

WINDOWS FORENSICS

Оливера Секулић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду описан је процес форензике оперативног система Windows, у склопу кога су представљене и разне технике, алати и начини спровођења форензичке истраге над дигиталним доказима који су резултат рада оперативног система Windows. Поред тога, дате су теоријске основе Windows оперативног система и описана је студија случаја која демонстрира процес дигиталне форензике оперативног система Windows.*

Кључне речи: *Дигитална форензика, дигитални докази, форензика оперативног система Windows*

Abstract – *This work describes Windows operating system forensics and includes description of various tools, techniques and methods of conducting examination of digital evidence that is the result of the operating system's activities. In addition, the theoretical foundations of the Windows operating system itself are given. Also, a case study is described, which covers the process of digital forensics over the described example.*

Keywords: *Digital forensics, digital evidence, forensics of Windows operating system*

1. УВОД

Дигитална форензика или дигитална форензичка наука је грана форензичке науке која се фокусира на проналажење и прегледање материјала пронађеног у дигиталним уређајима. Првобитно је коришћена као синоним за компјутерску форензику, али се касније проширила на истрагу свих уређаја који чувају дигиталне податке. Оперативни систем садржи системски и апликативни софтвер који нуди различите функције корисницима. Неке од њих су: управљање процесором, меморијом, улазно/излазним уређајима, подацима и апликацијама, контрола приступа, бележење догађаја, конфигурација самог оперативног система, и многе друге. Као резултат извршавања ових функција, настају различити артефакти који могу бити од интереса за форензичку истрагу, а који ће бити описани у остатку рада.

Задатак овог рада је да опише теоријске основе оперативног система Windows, као и алате, технике и начин спровођења истраге над дигиталним доказима који су резултат рада оперативног система. Друго поглавље овог рада односи се на теоријске основе оперативног система Windows о чијем форензичком истраживању је и реч. Објашњено је шта представља Windows оперативни систем, његов историјски развој, као и кључне карактеристике које га одликују. У трећем поглављу обухваћене су технике које су специфичне за форензику оперативног система Windows, као и начин њиховог функционисања. Четврто поглавље односи се на неке од алата који се користе у циљу оптимизоване истраге над оперативним системом Windows. Пето поглавље овог рада односи се на студију случаја преко које је представљен један од више могућих поступака форензичке истраге, а која је везана за Windows оперативни систем. Шесто поглавље представља закључак, резиме целокупног рада.

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

2. WINDOWS ОПЕРАТИВНИ СИСТЕМ

Microsoft Windows представља породицу оперативних система, чији главни задатак је да управља хардвером, подацима, као и да извршава наредбе корисника. Као такав, оперативни систем обједињује разнородне делове рачунара у складну целину, сакривајући од корисника детаље функционисања оних делова који нису битни за коришћење рачунара.

Са једне стране, он управља деловима од којих се састоји рачунар, са циљем да они буду што целисходније употребљени, а са друге стране, оперативни систем ствара приступачно радно окружење за крајњег корисника [1].

2.1. Кључне функције Windows оперативног система

Кључне функције Windows оперативног система су: контрола хардвера (контролише хардвер прикључен на рачунар),

- контрола програма (Windows помаже у отварању и затварању програма и даје им део меморије рачунара како би им омогућио да раде),
- контрола приступа (контролише какав приступ рачунару имају различити корисници),
- контрола грешака (бави се грешкама и издаје једноставне поруке о грешкама),
- складиштење података (контролише складиштење података),
- комуникација (омогућава кориснику да комуницира са рачунаром преко тастатуре, миша, микрофона итд.),
- мултитаскинг (Windows промовише мултитаскинг омогућавајући кориснику да ради неколико ствари на рачунару одједном) и

- претрага и организација (садржи алатке за претрагу за лакши и бржи проналазак потребних ствари).

2.2. Предности Windows оперативног система

Неке од кључних предности Windows оперативног система су:

- погодност (сви облици Microsoft Windows-а имају нешто уобичајено у себи што клијентима олакшава прелазак на другу верзију оперативног система почебши од једног обрасца до другог),
- компатибилност (Windows је оперативни систем који је веома компатибилан са већином програма или уређаја који се дистрибуирају),
- погодност дизајна (интерфејс је уредан, функционалан и једноставан за коришћење, а дизајн се истиче јер је иновативан и визуелно пријатан),
- подршка за више уређаја (Windows се може носити на свим уређајима без икаквих проблема),
- софтверска подршка (Windows платформа је погодна за програмере софтвера и рачунарских игара) и
- подршка за нови хардвер (Windows има подршку за нови хардвер зато што ће практично сви произвођачи хардвера понудити подршку за најновију верзију Windows-а када изађу на тржиште са новим производом).

2.3. Архитектура Windows оперативног система

Архитектура Windows оперативног система представља слојевити систем који чине две главне компоненте: кориснички режим и режим језгра, односно кернел режим. Извршавање корисничких апликација одвија се у корисничком режиму, док процеси који припадају оперативном систему раде у режиму језгра (кернел режиму) [2].

2.4. Windows регистар

Windows регистар представља једну од есенцијалних компоненти Microsoft Windows оперативних система. Као такав, представља централну хијерархијску базу података намењену за складиштење информација које су неопходне за конфигурисање система за једног или више корисника, апликација и хардверских уређаја. Постоји много информација у регистру које говоре оперативном систему и апликацијама шта да раде, где да смештају орећене ствари, као и како да реагују на одређени стимуланс. Користи се за чување великог броја информација и поставки за софтверске програме, конфигурације оперативног система, корисничке преференције и још много тога [3].

2.5. Лог датотеке

Лог датотеке се користе, како за оптимизовање система, тако и за праћење понашања корисника, проналазак грешака у раду апликација, бележење обавештења, генерисање података који су корисни за истраживање активности малициозних програма и многих других активности. Апликација која се најчешће користи за преглед лог датотека назива се Event Viewer [4]. Три категорије у које су сврстане лог датотеке и информације о њима, унутар Event Viewer-а су:

- Application – у овој категорији се бележе догађаји који су евидентирани од стране апликација.
- System – сваки догађај евидентиран од стране оперативног система.
- Security – када је безбедносно евидентирање омогућено, ова категорија бележи догађаје који се односе на безбедност.

3. ФОРЕНЗИЧКЕ ТЕХНИКЕ

3.1. Анализа Windows регистра

Windows регистар користи се за чување великог броја информација, конфигурације оперативног система, поставки за софтверске програме и још много тога, па самим тим представља и један од главних извора података који се анализира приликом форензичке истраге оперативног система Windows. За форензичког аналитичара, Windows регистар је „кутија са благом“. Служи као спремиште, надгледа, посматра и бележи активности које корисник обавља на рачунару. Постоји неколико начина за интеракцију са подацима и њихово издвајање из регистра. Један од њих јесте Registry Editor.

3.2. Анализа лог датотека

Анализа лог датотека Windows оперативног система је веома битна из перспективе дигиталне форензике из разлога што се ту чува сваки догађај који се догоди у оперативном систему. Са форензичке тачке гледишта, анализа лог датотека обухвата много података, а који су веома важни за форензичку истрагу. Тип догађаја који се снима може бити било која појава која утиче на систем: неуспешан покушај пријаве, модификација системских поставки, грешка апликације, квар система, коришћење ресурса као што су креирање, отварање или брисање датотека итд. Такође, веома је важна јер помаже у поновном креирању временске линије догађаја, како би се помогло у форензичкој истрази. Добра анализа и филтрирање лог датотека може дигиталног форензичара усмерити на прави пут у истрази и указати на то када су се десили неки догађаји релевантни за истрагу као и ко је изазвао те догађаје.

3.3. Анализа prefetch фајлова

Програмери који раде на одржавању оперативног система Windows, одувек су били заинтересовани за убразани процес покретања оперативног система и често коришћених програма. У ту сврху, Microsoft је дошао на идеју да се посвети праћењу података и библиотека које већина апликативних програма користи при покретању и њиховом чувању у таквом формату, да оперативни систем може лако да их учита у меморију пре него што заиста постану потребни. Од тада, сваки пут када се покрене нови програм у Windows-у, добија се унапред креирана датотека (енг. prefetch file), да убрза време следећег покретања програма. Сада, када постоји таква погодност, јавља се потреба за испитивањем безбедности и применом форензике ових датотека. Поред основних ставки које садржи у себи, prefetch фајлови садрже велики корпус података у којима се налази упутство за учитавање

онога што програм највише користи приликом свог покретања.

3.4. Преглед кластера

У оквиру Windows оперативног система, датотеке које се креирају у различитим дужинама у зависности од њиховог садржаја, чувају се у блоковима података фиксне дужине који се називају кластери. Веома ретко се величине датотека савршено подударају са величином једног или више кластера. Простор за складиштење података који постоји од краја датотеке до краја последњег кластера додељеног датотеци назива се „file slack“. Будући да file slack потенцијално садржи податке извучене насумично из меморије рачунара, могуће је идентификовати корисничка имена, лозинке и друге поверљиве информације повезане са коришћењем рачунара. На великим хард дисковима може укључивати неколико стотина мегабајта података. Такође, фрагменти ранијих е-маил порука и докумената за обраду текста се могу наћи унутар file slack-а. Са становишта дигиталне форензике, file slack је веома важан као извор дигиталних доказа унутар Windows оперативног система.

3.5. Swap датотека

Windows оперативни систем користи, за складиштење података из RAM-а, одређену датотеку под називом swap file. Њена функција јесте да обезбеди простор за складиштење података који припадају RAM-у, уколико је простор RAM-а пун. Знатно је већа од кластера, па је због тога већа вероватноћа добијања дигиталних доказа, унутар Windows оперативног система.

4. ФОРЕНЗИЧКИ АЛАТИ

4.1. ENCASE

EnCase алат се сматра водећим комерцијалним алатом за дигиталну форензику Windows оперативног система. Сматра се једним од најбољих и најчешће употребљаваних софтверских форензичких алата [5]. Основне карактеристике су:

- Прилагођен је форензичким истрагама на великим количинама података
- Омогућава прикупљање, прегледање и анализу доказа на Windows оперативином систему
- Обезбеђује физичко и логичко прикупљање података
- Верификован је

4.2. X-Ways Forensic алат

Неке од значајнијих карактеристика које X-Ways алат нуди укључују аутоматско откривање изгубљених или избрисаних партиција, читање партиција унутар слика масовне меморије и анализу удаљених рачунара [6]. Поред наведених, такође има и следеће карактеристике:

- Клонирање и креирање слике диска
- Приступ логичкој меморији покренутих процеса
- Различите технике опоравка података
- Омогућава прегледање и уређивање бинарних структура података помоћу шаблона

4.3. FTK Imager

Неке од карактеристика форензичког алата FTK Imager су:

- Омогућава креирање форензичке слике локалних чврстих дискова, CD-ова и DVD-ова, флеш дискова или других USB уређаја, читавих фасцикли или појединачних датотека са различитих места у медијима
- Омогућава преглед датотека и фасцикли на локалним чврстим дисковима, CD-овима и DVD-овима, флеш дисковима, мрежним дисковима или другим USB уређајима
- Омогућава преглед форензичких слика ускладиштених на локалној машини или на мрежном диску

4.4. Autopsy + The Sleuth Kit

Неке од карактеристика овог алата које су везане за Windows оперативни систем су:

- Ефикасно идентификовање активности користећи графички интерфејс
- Груписање датотека према њиховом типу, ради лакшег проналажења докумената и слика
- Могућност ознаке датотека произвољним именима ознака
- Помаже у означавању датотека и фолдера на основу путање и имена

Autopsy форензички алат је бесплатан. Како се буџети смањују, исплатива дигитална форензичка решења су од суштинског значаја. Такође, овај алат нуди исте основне карактеристике као и други дигитални форензички алати и нуди друге битне карактеристике као што су анализа веб артефаката, као и анализу регистра које други комерцијални алати не пружају [7].

4.5. Volatility

Volatiliy је алат отвореног кода који се користи у дигиталној форензици меморије Windows оперативног система. Овај алат прегледа и издваја меморијске артефакте 32-битних и 64-битних система из нестабилне меморије [8]. Неке од карактеристика Volatility алата су:

- Садржи команду за излиставање покренутих процеса
- Брзи и ефикасни алгоритми
- Омогућава анализу RAM-а на великим системима без непотребних трошкова или потрошње меморије
- Подржава различите формате датотека

5. СТУДИЈА СЛУЧАЈА

У овом примеру, представљен је студија случаја у којој је трговац, који ради у златари, украо накит и окривио особу која није одговорна за то дело. Какко би се утврдила истинитост дате ситуације, полиција даје налог за обуставу рада златаре и врши истрагу

над рачунаром, над којим су забележени записи које су снимиле камере.

5.1. Идентификација доказа

Ова фаза дигиталне форензике односи се на детектовање, препознавање и одређивање потенцијалних доказа које је потребно прикупити, сачувати, прегледати, анализирати и презентовати. Све што изгледа као потенцијални извор доказа се фотографише или снима, а такође и бележи, што ће послужити у каснијим корацима истраге.

5.2. Прикупљање доказа

Фаза прикупљања односи се на прикупљање података са дигиталних уређаја, правећи дигиталну копију података. У наведеном кривичном делу, истражитељи, након детектовања рачунара, пажљиво приступају рачунару и започињу фазу прикупљања, у овом случају то чине користећи Autopsy алат.

5.3. Прегледање доказа

Сви подаци који су прикупљени су подељени у више пакета унутар Autopsy алата, односно, у више категорија по којима се може вршити преглед.

5.4. Анализа доказа

Овај корак служи за обраду прикупљених података и самим тим одређивање чињеница о самом догађају, као и значају самих доказа и особа које су одговорне за исти, коришћењем специјалних алата.

5.5. Презентација доказа

Презентација доказа обухвата процес у којем форензичар дели резултате фазе анализе доказа у форми извештаја заинтересованим странама. Подаци који су релевантни се, на крају истраге, чувају и складиште на пажљив начин ради могуће касније употребе у даљим правним поступцима.

6. ЗАКЉУЧАК

Истражитељи који учествују у дигиталној форензици Windows оперативног система суочиће се са разним изазовима у будућности, међу којима је раст домета и броја уређаја које морају да провуку кроз истрагу, чиме се отежава форензичка истрага. Такође, долази до све већег броја злонамерног софтвера и метода крековања које напредују тако брзо да је истражитељима тешко да буду у току са новим методама. Поред наведених, постоји велика вероватноћа да ће бити и других изазова, али ће такође бити и евидентни напредак како алата тако и техника за спровођење дигиталне форензике.

7. ЛИТЕРАТУРА

[1] Per Brinch Hansen, Operating system principles, California Institute of Technology, Englewood Cliffs, New Jersey, 2001.

[2] Microsoft, Windows Hardware Developer, User mode and kernel mode, Article 2021, [online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode.

[3] Harlan Carvey, Windows Registry Forensics, Advanced Digital Forensic Analysis of the Windows Registry, pp. 1-27, USA, 2011.

[4] Lucideus, Introduction to Event Log Analysis Part 1 – Windows Forensics Manual 2018, Oct 26,2018. [online]. Available: https://medium.com/@lucideus/introduction-to-event-log-analysis-part-1-windows-forensics-manual-2018-b936a1a35d8a.

[5] OpenText EnCase Forensic, [online]. Available: https://security.opentext.com/encase-forensic.

[6] X-Ways Forensics: Integrated Computer Forensics Software, [online]. Available: http://www.x-ways.net/forensics/.

[7] Autopsy, [online]. Available: https://www.sleuthkit.org/autopsy/.

[8] Volatility Framework – Advanced Memory Forensics Framework, September 26,2016., [online]. Available: https://www.darknet.org.uk/2016/09/volatility-framework-advanced-memory-forensics-framework/.

Кратка биографија:

Оливера Секулић рођена је у Врбасу 1997. године. Завршила је основну школу „Иса Бајић“ у Кули и гимназију „Петро Кузмјак“ у Руском Крстуру, општи смер. Школске 2016/2017. године уписује Факултет техничких наука у Новом Саду, смер Рачунарство и аутоматика.