



ANÁLISIS FORENSE

Unidad 1. Actividad 8



22 DE ENERO DE 2023
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Driver Game Quiz.	1
------------------------	---

Driver Game Quiz.

1. A fin de que los abogados de la mafia no puedan alegar que se ha roto la cadena de custodia, comprueba que la evidencia no ha sufrido alteraciones. Haz esto tanto con PowerShell como con Autopsy.

Con powershell:

```
Sin título1.ps1 X
1 # Ruta del archivo
2 $rutaArchivo = "E:\Carlos\Ciberseguridad\ExamenForense\ExamenForense.img"
3
4 # Valor hash conocido (sustituye con tu propio valor)
5 $hashConocido = "e4216bb636648b7a4188aacef3587c64aabfb05aade76b6070b3ce8d66d4568a"
6
7 # Calcular el hash del archivo
8 $hashActual = Get-FileHash -Path $rutaArchivo -Algorithm SHA256 | Select-Object -ExpandProperty Hash
9
10 # Comparar los hashes
11 if ($hashActual -eq $hashConocido) {
12     Write-Host "El archivo no ha sufrido alteraciones."
13 } else {
14     Write-Host "El archivo ha sido alterado."
15 }
16 }
```

```
-a----      17/10/2023      19:02      1258 PilarMicro.lnk
-a----      22/01/2024      19:13      555 Sin título1.ps1
-a----      02/10/2023      11:52         0 tarea.txt

PS C:\Users\cdiaz\Desktop> & '.\Sin título1.ps1'
El archivo no ha sufrido alteraciones.
```

Otra forma de hacerlo:

```
PS C:\Users\cdiaz> Get-FileHash -Algorithm SHA256 "E:\Carlos\Ciberseguridad\ExamenForense\ExamenForense.img"
```

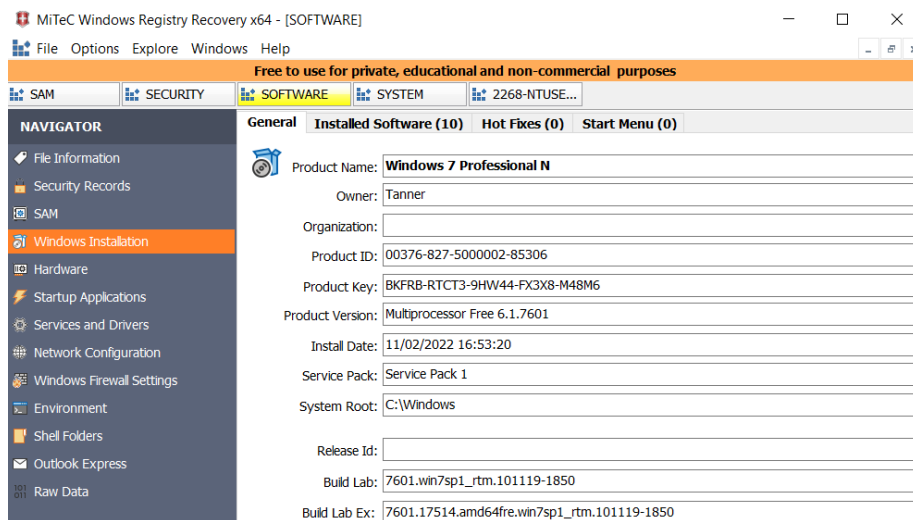
Algorithm	Hash	Path
SHA256	E4216BB636648B7A4188AAECF3587C64AABFB05AADE76B6070B3CE8D66D4568A	E:\Carlos\Ciberseguridad\Exam...

Con autopsy:

2. Comprueba que Tanner tiene un usuario en el equipo, y cuándo hizo login por última vez. Haz esto tanto en Autopsy como en Windows Registry Recovery.

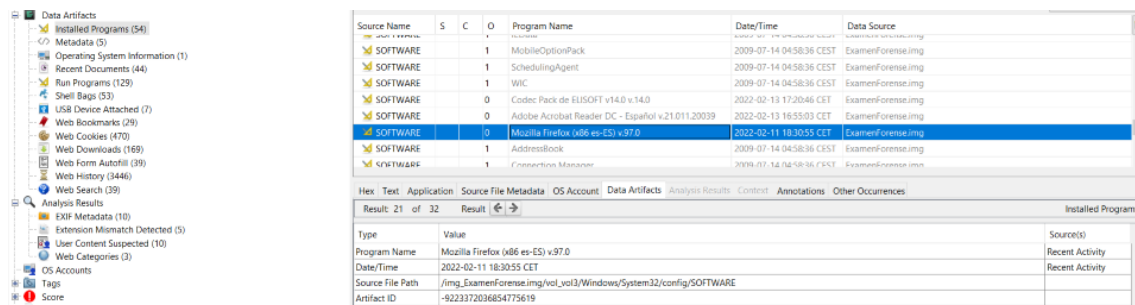
Con autopsy:

Con WRR:

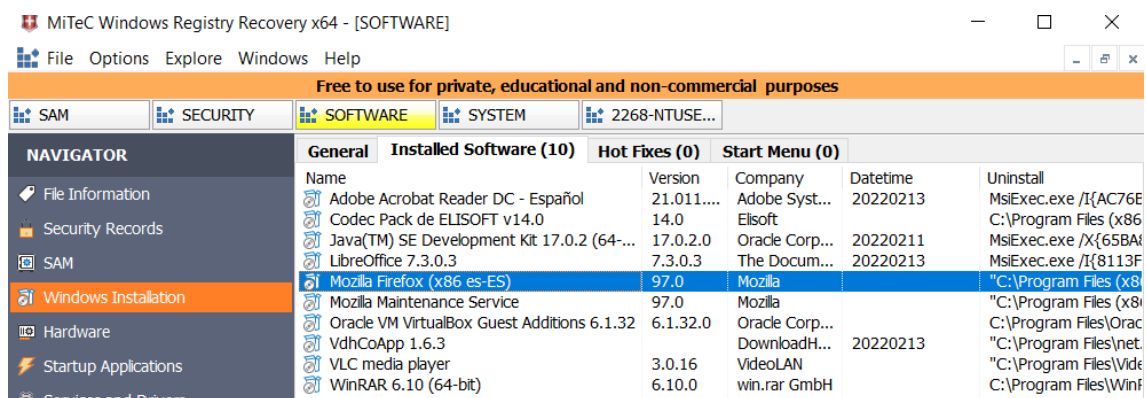


4. Por seguridad, Tanner ha instalado en el sistema un navegador web que no es de Microsoft. Consigue pruebas de cuál es y de que ha sido instalado. Haz esto tanto en Autopsy como en Windows Registry Recovery.

Esto se encuentra en el apartado de installer programs:



Con WRR:



5. Comprueba que Tanner sólo introdujo un pendrive en el equipo, porque debería ser el pendrive en el que se creó la imagen de memoria con DumpIt. ¿Cuál es dicho pendrive y a qué hora lo introdujo?

Con Autopsy:

USB Device Attached

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM		1		2022-02-11 17:51:14 CET	ROOT_HUB		462466eb65b0	ExamenForens...img
SYSTEM		1		2022-02-11 17:51:14 CET	ROOT_HUB20		466a987e4d0	ExamenForens...img
SYSTEM		1		2022-02-11 17:51:15 CET	VirtualBox	USB Tablet	5818f54cb78081	ExamenForens...img
SYSTEM		1		2022-02-13 18:26:03 CET	ROOT_HUB		462466eb65b0	ExamenForens...img
SYSTEM		1		2022-02-12 14:39:17 CET	Kingston Technology	DataTraveler 100 G3/G4/S9 G2/50	002618525C8F080687D2853	ExamenForens...img
SYSTEM		1		2022-02-13 18:26:04 CET	VirtualBox	USB Tablet	5818f54cb78081	ExamenForens...img

USB Device Attached

Type	Value	Source(s)
Date/Time	2022-02-12 14:39:17 CET	Recent Activity
Device Make	Kingston Technology	Recent Activity
Device Model	DataTraveler 100 G3/G4/S9 G2/50	Recent Activity
Device ID	002618525C8F080687D2853	Recent Activity
Source File Path	/img_ExamenForens...img/vol_x013/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775663	

6. Tanner ha accedido a un fichero con extensión .doc recientemente ¿En qué fecha y hora fue accedido?

Recent Documents

Source Name	S	C	O	Path	Date Accessed	Data Source
Mis imágenes.Ink				C:\Users\Tanner\Pictures	2022-02-13 19:09:53 CET	ExamenFor...
O Anarquismo no Século XXI e outros Ensaios by David Graeber (z-lib.org).Ink				C:\Users\Tanner\Downloads\O Anarquismo no S-culo XXI e o	2022-02-13 17:54:41 CET	ExamenFor...
personal-monthly-budget.Ink				C:\Users\Tanner\Downloads\personal-monthly-budget.xlsx	2022-02-13 18:23:07 CET	ExamenFor...
problemas.Ink				C:\Users\Tanner\Downloads\problemas.txt	2022-02-13 18:24:15 CET	ExamenFor...
Walden La Vida En Los Bosques by Thoreau, Henry David (z-lib.org).Ink				C:\Users\Tanner\Documents\Walden La Vida En Los Bosques	2022-02-13 17:58:53 CET	ExamenFor...
Koala.jpg.Ink				C:\Users\Public\Pictures\Sample Pictures\Koala.jpg	0000-00-00 00:00:00	ExamenFor...
No preferred path found.Ink				No preferred path found	0000-00-00 00:00:00	ExamenFor...

Recent Documents

Type	Value	Source(s)
Path	C:\Users\Tanner\Documents\Walden La Vida En Los Bosques by Thoreau, Henry David (z-lib.org).doc	RecentActivity
Path ID	-1	RecentActivity
Date Accessed	2022-02-13 17:58:53 CET	RecentActivity
Source File Path	/img_ExamenForens...img/vol_x013/Users/Tanner/AppData/Roaming/Microsoft/Windows/Recent/Walden La Vida En Los Bosques by Thoreau, Henry Dav	
Artifact ID	-9223372036854775761	

7. Tanner ha estado buscando información sobre un afamado terrorista. En concreto, ha estado viendo vídeos sobre él en una plataforma online. ¿Quién es dicho terrorista?

The screenshot shows the ExaminForensic tool interface. The left sidebar displays a tree view of data sources, including 'ExamForensic.img_1 Host' and 'ExamForensic.img'. The main window shows a 'Listing' tab with a table of search results. The table has columns: Source Name, S, C, O, Domain, Text, Program Name, Date Accessed, and Data Source. The results are filtered by 'unabombert' and show several entries from 'places.sqlite' files, including 'unabombert' from 'youtube.com'.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
places.sqlite				google.com	code: pack elisof	Firefox Analyzer	2022-02-13 17:40:12 CET	ExamForensic.img
places.sqlite				google.com	vlc	Firefox Analyzer	2022-02-13 17:40:51 CET	ExamForensic.img
places.sqlite				google.com	video download helper	Firefox Analyzer	2022-02-13 17:42:16 CET	ExamForensic.img
places.sqlite				youtube.com	unabombert	Firefox Analyzer	2022-02-13 17:42:54 CET	ExamForensic.img
places.sqlite				youtube.com	unabomber	Firefox Analyzer	2022-02-13 17:42:57 CET	ExamForensic.img
places.sqlite				google.com	ted kaczynski manifesto	Firefox Analyzer	2022-02-13 17:47:00 CET	ExamForensic.img
places.sqlite				google.com	ted kaczynski manifesto pdf	Firefox Analyzer	2022-02-13 17:47:07 CET	ExamForensic.img
places.sqlite				google.com	libros en pdf	Firefox Analyzer	2022-02-13 17:47:57 CET	ExamForensic.img

The 'Web Search' section below the table shows the search term 'unabombert', time '2022-02-13 17:42:54 CET', domain 'youtube.com', and program name 'Firefox Analyzer'. The 'Source' section shows the host 'ExamForensic.img_1 Host', data source 'ExamForensic.img', and file path '/img_ExamenForensic.img/vol_vol3/Users/Tanner/AppData/Roaming/Mozilla/Firefox/Profiles/2og5kq0l.default-release/places.sqlite'.

8. Para acabar con Jean Paul, Tanner ha adquirido un arma. ¿Sobre qué arma en concreto ha buscado información?

The screenshot shows the ExaminForensic tool interface. The left sidebar displays a tree view of data sources, including 'ExamForensic.img_1 Host' and 'ExamForensic.img'. The main window shows a 'Listing' tab with a table of search results. The table has columns: Source Name, S, C, O, Domain, Text, Program Name, Date Accessed, and Data Source. The results are filtered by 'smith and wesson 9mm' and show several entries from 'places.sqlite' files, including 'smith and wesson 9mm' from 'google.com'.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
places.sqlite				google.com	libreoffice	Firefox Analyzer	2022-02-13 17:49:14 CET	ExamForensic.img
places.sqlite				google.com	adobe reader	Firefox Analyzer	2022-02-13 17:49:32 CET	ExamForensic.img
places.sqlite				google.com	smith and wesson 9mm	Firefox Analyzer	2022-02-13 18:04:14 CET	ExamForensic.img
places.sqlite				youtube.com	dragon ball	Firefox Analyzer	2022-02-13 18:04:59 CET	ExamForensic.img
places.sqlite				youtube.com	dr slump galego	Firefox Analyzer	2022-02-13 18:05:25 CET	ExamForensic.img
places.sqlite				youtube.com	detective conan galego	Firefox Analyzer	2022-02-13 18:05:46 CET	ExamForensic.img
places.sqlite				youtube.com	xabarin club	Firefox Analyzer	2022-02-13 18:06:06 CET	ExamForensic.img
places.sqlite				qoogle.com	new york times	Firefox Analyzer	2022-02-13 18:11:36 CET	ExamForensic.img

The 'Web Search' section below the table shows the search term 'smith and wesson 9mm', time '2022-02-13 18:04:14 CET', domain 'google.com', and program name 'Firefox Analyzer'. The 'Source' section shows the host 'ExamForensic.img_1 Host', data source 'ExamForensic.img', and file path '/img_ExamenForensic.img/vol_vol3/Users/Tanner/AppData/Roaming/Mozilla/Firefox/Profiles/2og5kq0l.default-release/places.sqlite'.

9. Tanner se aloja en el Holiday Inn Manhattan Financial District, pero Jean Paul está alojado en otro hotel diferente. Tanner tiene planeado ir a buscarlo en su coche. ¿En qué hotel se aloja Jean Paul?

Web History

3446 Results

Table	Thumbnail	Summary				Save Table as CSV
	Date Accessed	Referrer URL	Title	Program Name	Domain	
ps	2022-02-13 18:01:46 CET	http://maps.google.es/maps	Google Maps	Firefox Analyzer	google.	
ps/@43.4864686,-8.2099258,	2022-02-13 18:01:52 CET	https://www.google.es/maps	Hilton Garden Inn New York/Central Park South-Midtown	Firefox Analyzer	google.	
ps/place/Hilton+Garden+Inn,	2022-02-13 18:02:08 CET	https://www.google.es/maps/@43.4864686,-8.2099258,1	Hilton Garden Inn - Google Maps	Firefox Analyzer	google.	
ps/place/Hilton+Garden+Inn,	2022-02-13 18:02:10 CET	https://www.google.es/maps/place/Hilton+Garden+Inn,	Google Maps	Firefox Analyzer	google.	
ps/dir//Hilton+Garden+Inn,+	2022-02-13 18:03:00 CET	https://www.google.es/maps/place/Hilton+Garden+Inn,	Google Maps	Firefox Analyzer	google.	
ps/dir/Holiday+Inn+Manhatt,	2022-02-13 18:03:13 CET	https://www.google.es/maps/dir//Hilton+Garden+Inn,+	de Holiday Inn Manhattan-Financial District a Hilton Gar	Firefox Analyzer	google.	
ps/dir/Holiday+Inn+Manhatt,	2022-02-13 18:03:17 CET	https://www.google.es/maps/dir/Holiday+Inn+Manhatt,	de Holiday Inn Manhattan-Financial District a Hilton Gar	Firefox Analyzer	google.	
< >						
Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	
Analysis Results Context Annotations Other Occurrences						
Result: 91	of 203	Result				
Web History						
Visit Details						
Title:	Hilton Garden Inn New York/Central Park South-Midtown West, West 54th Street, Nueva York, EE. UU. - Google Maps					
Date Accessed:	2022-02-13 18:01:52 CET					
Domain:	google.es					
URL:	https://www.google.es/maps/@43.4864686,-8.2099258,15z					
Referrer URL:	https://www.google.es/maps					
Program Name:	Firefox Analyzer					
Source						
Host:	ExamenForense.img_1 Host					
Data Source:	ExamenForense.img					
File:	/img_ExamenForense.img/vol_vol3/Users/Tanner/AppData/Roaming/Mozilla/Firefox/Profiles/2og5kq0l.default-release/places.sqlite					

10. Tras acabar la misión, Tanner tiene pensado ir a otro lugar. ¿Cuál es dicho lugar y cómo tiene pensado ir?

Esta buscando un vuelo de New York a Cancun:

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
🔍 places.sqlite				google.com	vuelos new york cancun	FireFox Analyzer	2022-02-13 18:13:35 CET	ExamenForense.img
🔍 places.sqlite				google.com	vertex42 personal monthly budget	FireFox Analyzer	2022-02-13 18:22:51 CET	ExamenForense.img
🔍 index.dat				bing.com	download firefox	Internet Explorer Analyzer	2022-02-11 18:27:25 CET	ExamenForense.img
🔍 index.dat				bing.com	jdk download	Internet Explorer Analyzer	2022-02-11 18:27:37 CET	ExamenForense.img
🔍 index.dat				bing.com	download firefox	Internet Explorer Analyzer	2022-02-11 18:26:09 CET	ExamenForense.img
🔍 index.dat				bing.com	jdk download	Internet Explorer Analyzer	2022-02-11 18:27:31 CET	ExamenForense.img
🔍 index.dat				bing.com	download firefox	Internet Explorer Analyzer	2022-02-11 18:26:08 CET	ExamenForense.img
🔍 index.dat				bing.com	jdk download	Internet Explorer Analyzer	2022-02-11 18:27:31 CET	ExamenForense.img

HexTextApplicationSource File MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

Result: 202 of 203Result↩️➡️Web Search

Web Search

Term:vuelos new york cancun

Time:2022-02-13 18:13:35 CET

Domain:google.com

Program Name:FireFox Analyzer

Source

Host:ExamenForense.img_1 Host

Data Source:ExamenForense.img

File:/img_ExamenForense.img/vol_vol3/Users/Tanner/AppData/Roaming/Mozilla/Firefox/Profiles/2og5kq0l.default-release/places.sqlite