



---

# ANÁLISIS FORENSE

---

Unidad 1. Actividad 9



27 DE ENEROE DE 2023  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

## Índice

Tarea evaluable de Análisis de disco .....	2
--	---

# Tarea evaluable de Análisis de disco

## 1. ¿Cuál es el nombre de usuario del equipo?

El usuario del equipo es Pacopepe

/img\_imagen.img/vol\_vol3/Users 8 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	k
[current folder]				2022-04-05 14:34:53 CEST	2022-04-05 14:34:53 CEST	2022-05-18 19:30:59 CEST	2019-12-07 10:03:44 CET	56	Allocated	Allocated	u
[parent folder]				2022-05-18 19:08:27 CEST	2022-05-18 19:08:27 CEST	2022-05-18 19:31:07 CEST	2019-12-07 10:03:44 CET	56	Allocated	Allocated	u
All Users				2019-12-07 10:25:05 CET	2022-04-05 15:05:06 CEST	2019-12-07 10:25:05 CET	2019-12-07 10:25:05 CET	48	Allocated	Allocated	u
Default				2022-04-05 14:18:00 CEST	2022-04-05 14:18:00 CEST	2022-04-27 19:33:35 CEST	2019-12-07 10:03:44 CET	160	Allocated	Allocated	u
Default User				2019-12-07 10:25:05 CET	2022-04-05 15:05:06 CEST	2019-12-07 10:25:05 CET	2019-12-07 10:25:05 CET	48	Allocated	Allocated	u
Pacopepe				2022-04-26 01:31:14 CEST	2022-04-26 01:31:14 CEST	2022-05-18 19:30:59 CEST	2022-04-05 14:26:07 CEST	176	Allocated	Allocated	u
Public				2022-04-05 14:27:18 CEST	2022-04-05 14:27:18 CEST	2022-05-18 19:24:06 CEST	2019-12-07 10:14:16 CET	56	Allocated	Allocated	u
desktop.ini				2019-12-07 10:12:11 CET	2022-04-05 14:48:10 CEST	2022-05-18 19:30:47 CEST	2019-12-07 10:14:18 CET	174	Allocated	Allocated	u

## 2. ¿Qué personaje público es el posible objeto del atentado?

Por las ultimas cosas que ha buscado podemos concluir que es Feijo:

Lisung Web Search 79 Results

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
places.sqlite				google.com	feijoo	FireFox Analyzer	2022-05-04 20:00:06 CEST	imagen.img
places.sqlite				google.com	feijoo hoy	FireFox Analyzer	2022-05-04 20:00:09 CEST	imagen.img
places.sqlite				google.com	hoteles madrid	FireFox Analyzer	2022-05-04 20:01:26 CEST	imagen.img
places.sqlite				google.com	minijuegos	FireFox Analyzer	2022-05-04 20:24:52 CEST	imagen.img
places.sqlite				google.com	accesos palacio moncloa	FireFox Analyzer	2022-05-06 18:58:19 CEST	imagen.img
places.sqlite				google.com	accesos palacio moncloa	FireFox Analyzer	2022-05-06 18:58:23 CEST	imagen.img
places.sqlite				google.com	acceso moncloa	FireFox Analyzer	2022-05-06 19:05:18 CEST	imagen.img
places.sqlite				google.com	acceso palacio moncloa	FireFox Analyzer	2022-05-06 19:08:03 CEST	imagen.img
places.sqlite				google.com	acceso palacio moncloa	FireFox Analyzer	2022-05-06 19:08:08 CEST	imagen.img
places.sqlite				google.com	acceso palacio moncloa	FireFox Analyzer	2022-05-06 19:08:10 CEST	imagen.img
places.sqlite				google.com	fabricación de bombas caseras	FireFox Analyzer	2022-05-06 19:18:00 CEST	imagen.img

## 3. ¿En qué lugar estaba el sospechoso planeando llevar a cabo el atentado?

En la Moncloa:

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
places.sqlite				google.com	feijoo	FireFox Analyzer	2022-05-04 20:00:06 CEST	imagen.img
places.sqlite				google.com	feijoo hoy	FireFox Analyzer	2022-05-04 20:00:09 CEST	imagen.img
places.sqlite				google.com	hoteles madrid	FireFox Analyzer	2022-05-04 20:01:26 CEST	imagen.img
places.sqlite				google.com	minijuegos	FireFox Analyzer	2022-05-04 20:24:52 CEST	imagen.img
places.sqlite				google.com	accesos palacio moncloa	FireFox Analyzer	2022-05-06 18:58:19 CEST	imagen.img
places.sqlite				google.com	accesos palacio moncloa	FireFox Analyzer	2022-05-06 18:58:23 CEST	imagen.img
places.sqlite				google.com	acceso moncloa	FireFox Analyzer	2022-05-06 19:05:18 CEST	imagen.img
places.sqlite				google.com	acceso palacio moncloa	FireFox Analyzer	2022-05-06 19:08:03 CEST	imagen.img
places.sqlite				google.com	acceso palacio moncloa	FireFox Analyzer	2022-05-06 19:08:08 CEST	imagen.img
places.sqlite				google.com	acceso palacio moncloa	FireFox Analyzer	2022-05-06 19:08:10 CEST	imagen.img
places.sqlite				google.com	fabricación de bombas caseras	FireFox Analyzer	2022-05-06 19:18:00 CEST	imagen.img

#### 4. ¿Cuáles serían los posibles alojamientos del sospechoso?

En un hotel de Madrid:

Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
places.sqlite	google.com	feijoo hoy	Firefox Analyzer	2022-05-04 20:00:09 CEST	imagen.img		
places.sqlite	google.com	hoteles madrid	Firefox Analyzer	2022-05-04 20:01:26 CEST	imagen.img		
places.sqlite	google.com	minijuegos	Firefox Analyzer	2022-05-04 20:24:52 CEST	imagen.img		

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 731 of 742 Result

Web Search

Term: hoteles madrid  
Time: 2022-05-04 20:01:26 CEST  
Domain: google.com  
Program Name: Firefox Analyzer

Source

Host: imagen.img\_1 Host  
Data Source: imagen.img  
File: /img\_imagen.img/vol\_vol3/Users/Pacopepe/AppData/Roaming/Mozilla/Firefox/Profiles/hgxy1vr2.default-release/places.sqlite

El hotel se llama:

Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
places.sqlite	google.com	feijoo hoy	Firefox Analyzer	2022-05-04 20:00:09 CEST	imagen.img		
places.sqlite	google.com	hoteles madrid	Firefox Analyzer	2022-05-04 20:01:26 CEST	imagen.img		
places.sqlite	google.com	minijuegos	Firefox Analyzer	2022-05-04 20:24:52 CEST	imagen.img		

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 365 of 742 Result

Web History

Visit Details

Title: Hotel Riu Plaza España, web oficial  
Date Accessed: 2022-05-04 20:01:39 CEST  
Domain: riu.com  
URL: https://www.riu.com/es/hotel/espana/madrid/hotel-riu-plaza-espana/?gclid=EAlaIQobChMI9Ln9z7bG9wVM09oCR1TvghDEAAyAAEgJN6vD\_BwE&gclid=aw.ds  
Referrer URL: https://ad.doubleclick.net/ddm/clk/437551470;240562172;au=ds&sv1=677845888678&sv2=3303374596812272&sv3=5440871775456896115&gclid=EAlaIQobChMI9Ln9z7bG9wVM09oCR1TvghDEAAyAAEgJN6vD\_BwE&gclid=aw.ds  
Program Name: Firefox Analyzer

#### 5. El sospechoso estuvo viendo un programa en YouTube que le ha motivado para llevar a cabo el atentado. ¿Cuál es dicho programa?

He encontrado varios canales de youtube, todos eran sobre música menos este:

Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
places.sqlite	youtube.com	los minutos del odio	Firefox Analyzer	2022-04-26 00:04:32 CEST	imagen.img		
places.sqlite	google.com	windows 10 desactivar bloqueo de pantalla	Firefox Analyzer	2022-04-27 16:24:57 CEST	imagen.img		
places.sqlite	youtube.com	puritanical euphoric misanthropia	Firefox Analyzer	2022-04-27 18:09:18 CEST	imagen.img		
places.sqlite	google.com	feijoo hoy	Firefox Analyzer	2022-04-28 17:51:53 CEST	imagen.img		

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 678 of 742 Result

Web Search

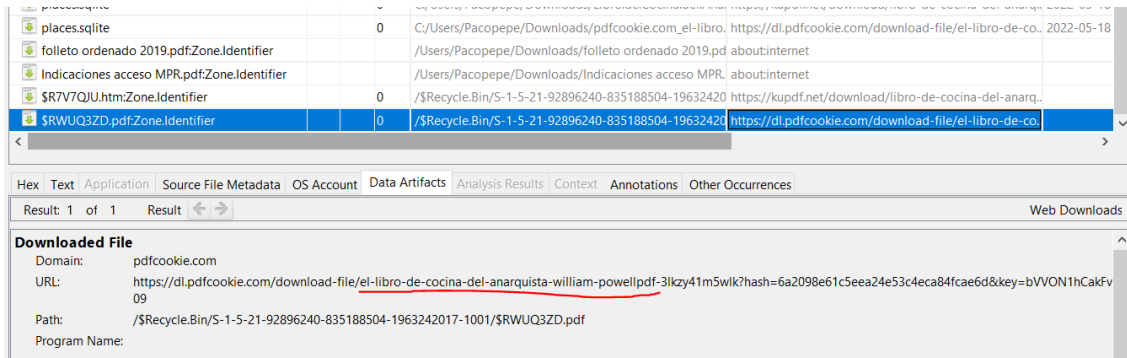
Term: los minutos del odio  
Time: 2022-04-26 00:04:32 CEST  
Domain: youtube.com  
Program Name: Firefox Analyzer

Source

Host: imagen.img\_1 Host  
Data Source: imagen.img  
File: /img\_imagen.img/vol\_vol3/Users/Pacopepe/AppData/Roaming/Mozilla/Firefox/Profiles/hgxy1vr2.default-release/places.sqlite

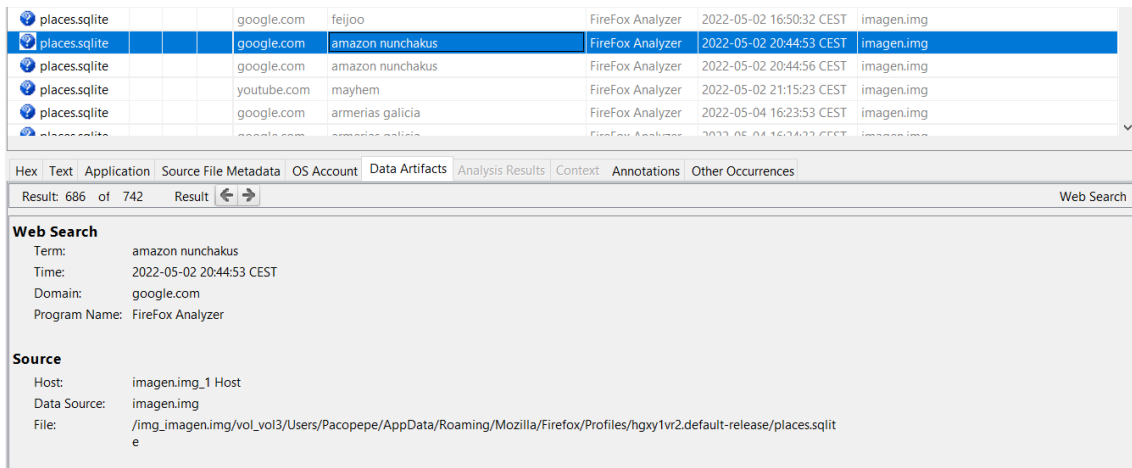
6. Además, el sospechoso ha estado leyendo un libro que le puede ayudar en el atentado. ¿Cuál es dicho libro?

El libro de cocina del anarquismo:

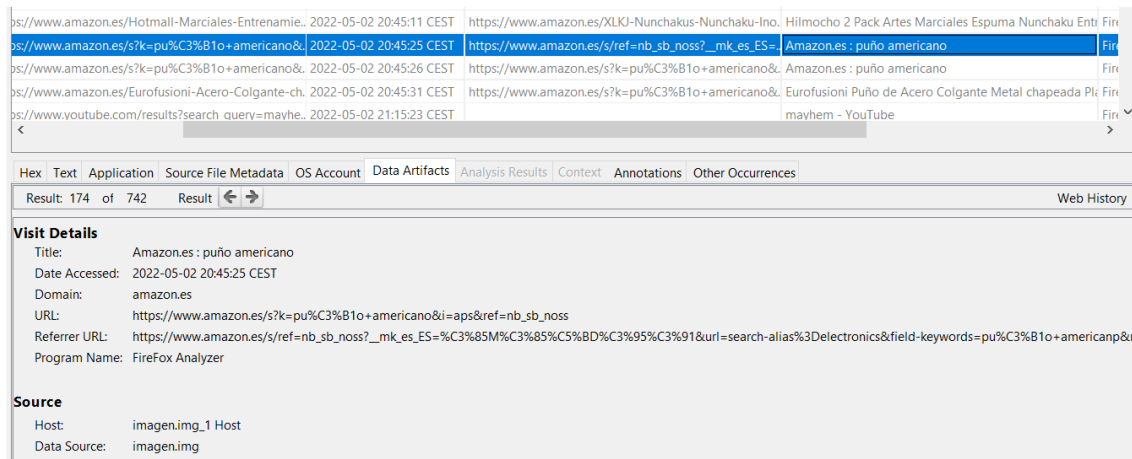


7. El sospechoso ha estado buscando armas en varias páginas de armerías de Galicia. Sin embargo, sólo ha anotado los precios del material de dos de las armerías que ha visitado. ¿Cuáles son dichas armerías?

Uno son los nunchakus:






El segundo es el puño americano:



## 8. ¿Existe alguna imagen cuyos metadatos EXIF nos puedan ayudar en el caso?

No he encontrado nada relevante:

EXIF Metadata											3 Results
Table Thumbnail Summary											
Save Table as CSV											
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Date Created	File Path	
 WelcomeScan.jpg				File	Not Notable				2004-04-09 08:17:00 CEST	/img_imagen.img/vol_03/ProgramData	
 bg1a_thumb.png				File	Not Notable				2017-09-27 16:05:12 CEST	/img_imagen.img/vol_03/Program Files	
 WelcomeScan.jpg				File	Not Notable				2004-04-09 08:17:00 CEST	/img_imagen.img/vol_03/Windows/Wir	