

TAREA 1: METADATOS Y ESTEGANOGRAFÍA



Eric Serrano Marín
CETI HACKING ETICO

ÍNDICE

FOCA Y EXIFTOOL	2
1. Realiza la instalación del software open source FOCA en tu máquina virtual Windows 10.	2
2. Agrega tu Google Api de búsqueda. Tienes un enlace a la sección de la wiki de FOCA en la plataforma.	3
3. Realiza una búsqueda de metadatos de algún fichero. Emplea FOCA y alguna alternativa como exiftool. Edita algún metadato del fichero, analiza y luego borralos. 6	
4. Crea un nuevo proyecto en FOCA denominado “Mi proyecto en FOCA”. Analiza algún dominio que proporcione variedad de archivos. Analízalos y saca un reporte del mismo.	10
ESTEGANOGRAFÍA	11
1. Oculta algún tipo de información en un archivo de tu elección. Prueba a extraerla.	11
2. Oculta algún tipo de información en un archivo protegido por contraseña. Realiza fuerza bruta para intentar obtener el archivo.	12
(Opcional): prueba las alternativas en desarrollo a StegCracker y realiza una comparativa de rendimiento.	12

FOCA Y EXIFTOOL

1. Realiza la instalación del software open source FOCA en tu máquina virtual Windows 10.

Explico el proceso así por encima, ya que antes de empezar esta práctica ya había hecho la instalación mientras seguía la clase.

- He descargado el zip de FOCA desde el repositorio, al darle al exe no funcionaba, nos pedía sql server.
- He instalado sql server,
- Después solo teníamos que añadir el localhost cuando daba error.

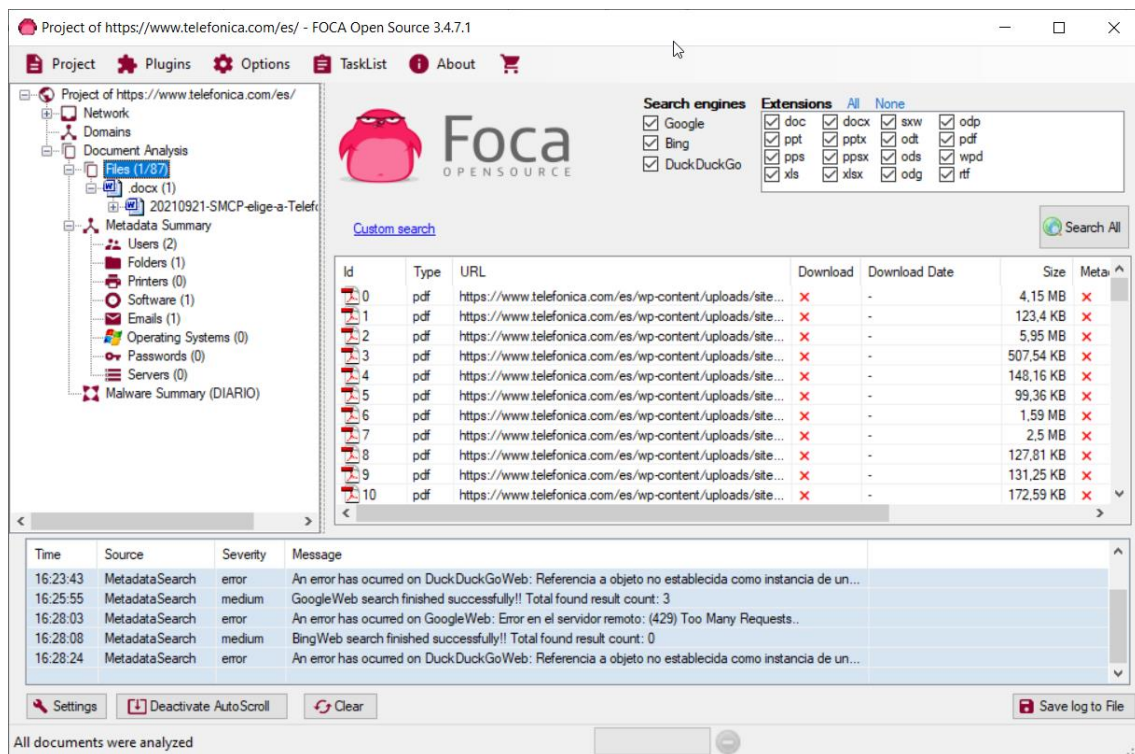


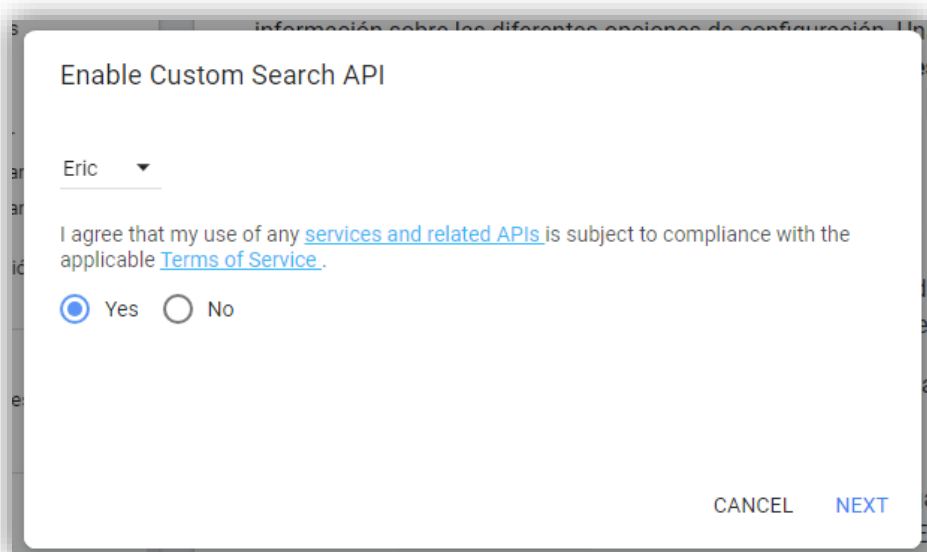
Ilustración 1 Prueba de la realización de instalación FOCA.

2. Agrega tu Google Api de búsqueda. Tienes un enlace a la sección de la wiki de FOCA en la plataforma.

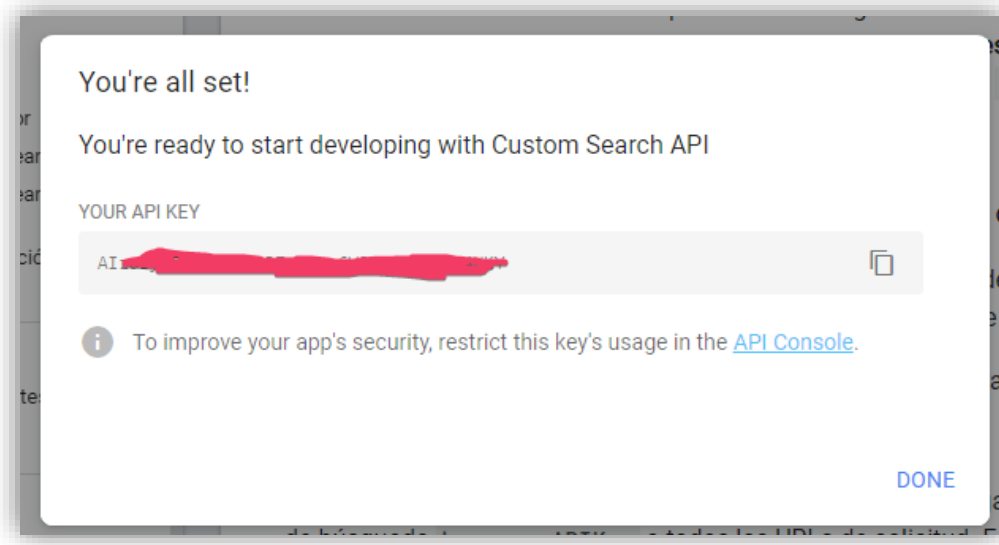
- Entramos en <https://developers.google.com/>
- Haremos clic en GET A KEY.



- Seguiremos al siguiente paso:

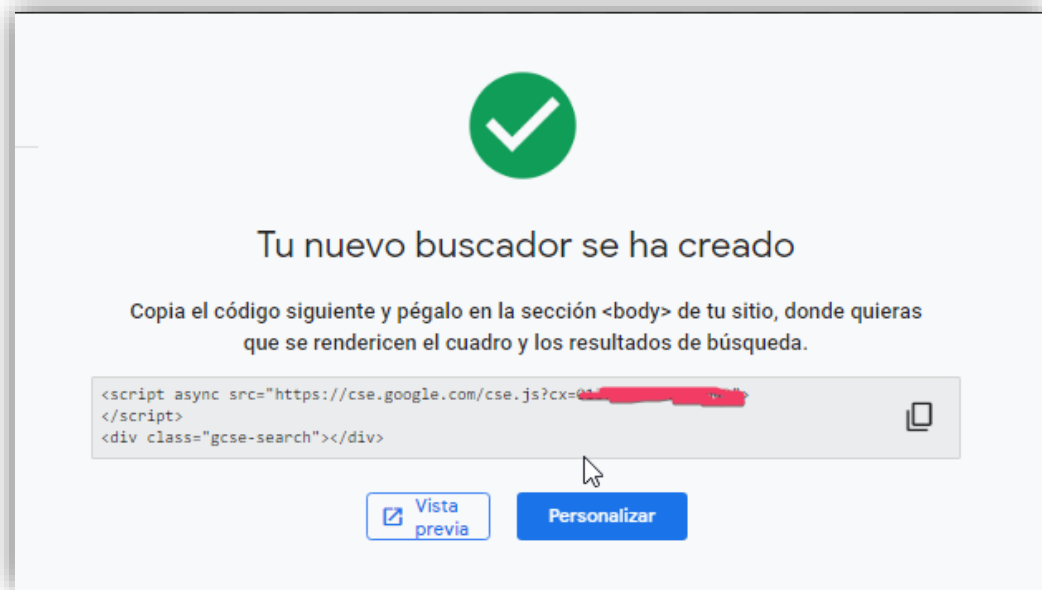


- Y ya tendremos nuestra key.

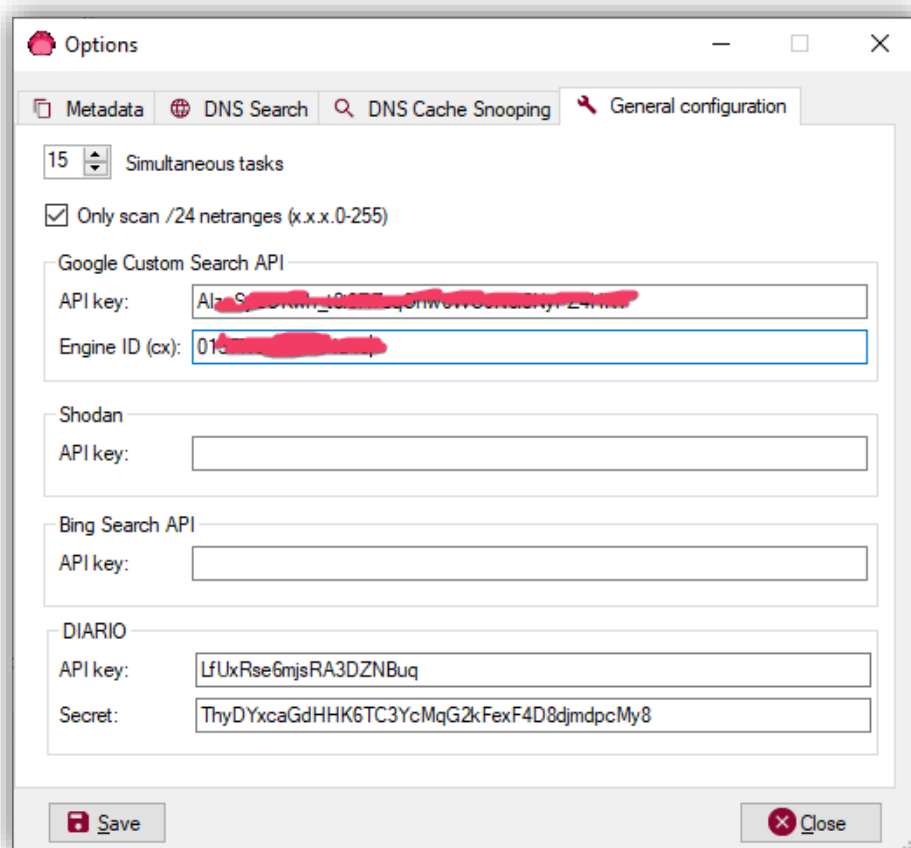


- Lo siguiente será irnos al siguiente enlace y rellenar:
<https://programmablesearchengine.google.com/controlpanel/create>

A screenshot of a web form titled "Crear un nuevo buscador". The form has several sections: 1. "Asigna un nombre a tu buscador" with a text input field containing "eric". 2. "¿Dónde buscar?" with a radio button selected for "Buscar sitios o páginas específicos". Below this, there is a list of examples for adding sites and a text input field with "Añadir" button. 3. "Configuración de búsqueda" with two toggle switches: "Búsqueda por imágenes" and "Búsqueda Segura", both currently turned off. 4. A reCAPTCHA checkbox labeled "No soy un robot". 5. A "Crear" button at the bottom. The form also includes a link to "Más información" and "Términos del Servicio".



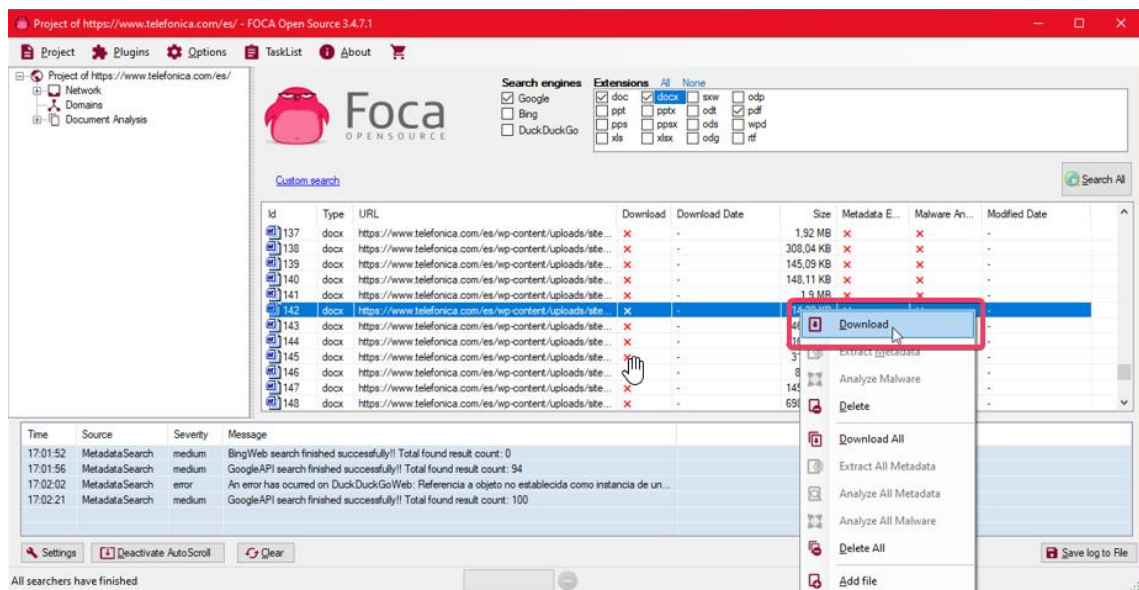
- Añadiremos la API KEY de los pasos anteriores y el Engine ID que es la sentencia de números que nos ha dado el nuevo buscador que hemos creado.



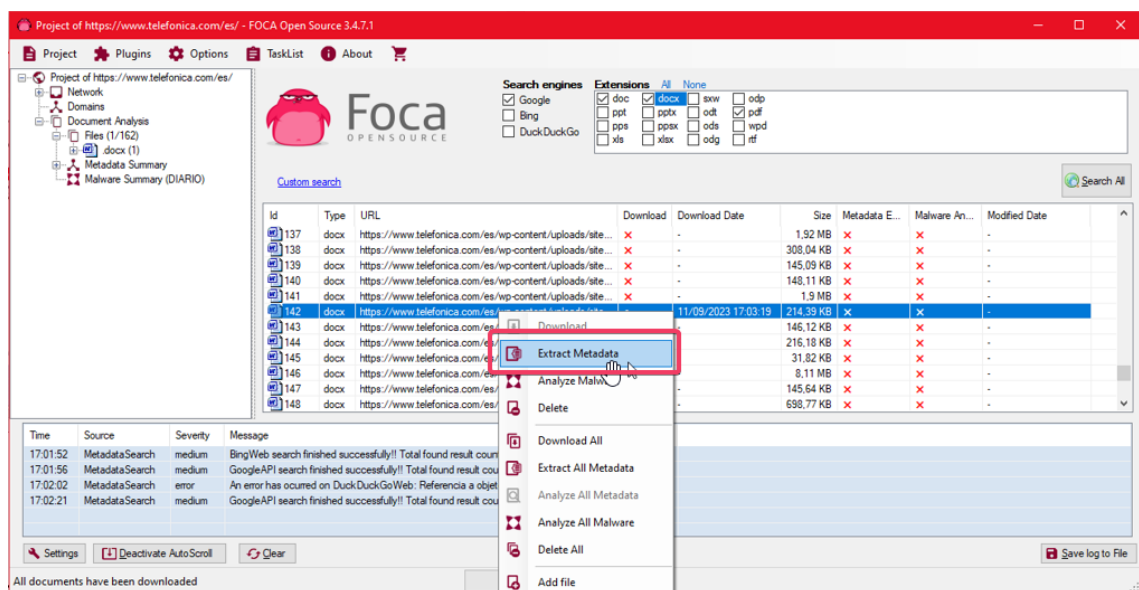
3. Realiza una búsqueda de metadatos de algún fichero. Emplea FOCA y alguna alternativa como exiftool. Edita algún metadato del fichero, analiza y luego borralos.

FOCA

En new Project hemos puesto <https://www.telefonica.com/es/>, y hemos puesto para buscar por pdf, doc y docx. Hemos elegido uno y hemos hecho clic derecho y descargar.

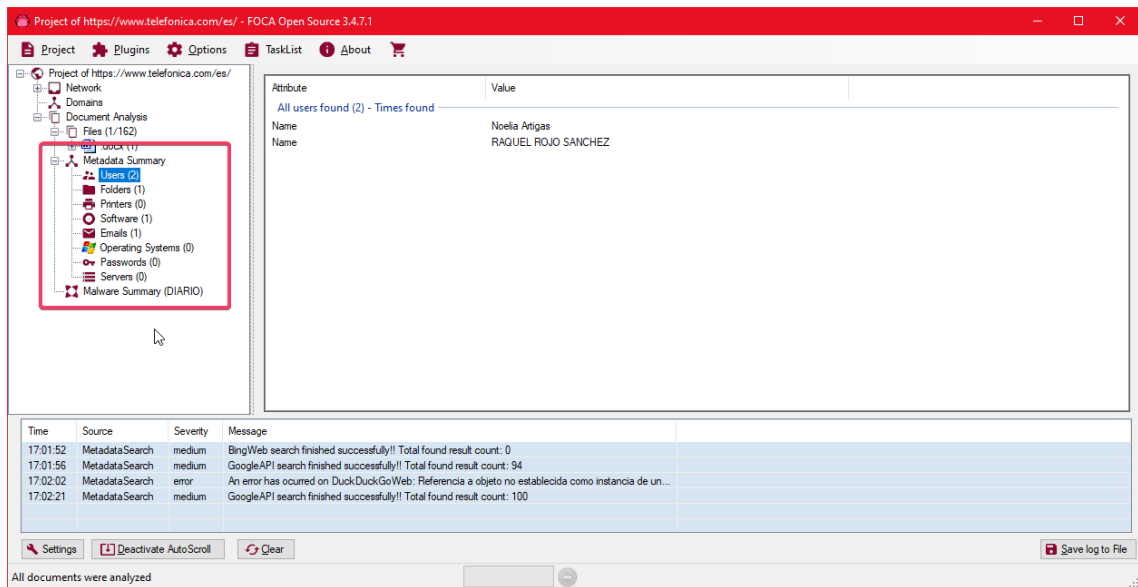


Clic derecho y extract metadata.



Ahí tenemos lo que ha encontrado:

- 2 usuarios (Noelia Artigas y Raquel Rojo Sanchez)
- En Folders ha encontrado una ruta.
- Software Microsoft Office.
- Y mails ha encontrado uno, que es mathilde.magnan@smcp.com



Con FOCA no podemos (hasta donde yo he encontrado) editar metadatos.

EXIFTOOL

Sacando metadatos del archivo de Amazon.

```
(kali㉿kali)-[~/Desktop]
└─$ exiftool Amazon-Complaint-\\(Dkt.1\\).pdf
ExifTool Version Number      : 12.67
File Name                    : Amazon-Complaint-(Dkt.1).pdf
Directory                   : .
File Size                    : 252 kB
File Modification Date/Time  : 2023:11:09 11:31:13-05:00
File Access Date/Time       : 2023:11:09 11:31:13-05:00
File Inode Change Date/Time  : 2023:11:09 11:31:13-05:00
File Permissions             : -rw-r--r--
File Type                   : PDF
File Type Extension         : pdf
MIME Type                   : application/pdf
PDF Version                 : 1.6
Linearized                  : Yes
Author                     : Federal Trade Commission
Create Date                : 2023:05:31 09:50:09-04:00
Modify Date                : 2023:05:31 14:53:45-04:00
Language                   : en
Tagged PDF                 : Yes
XMP Toolkit                 : Adobe XMP Core 9.1-c001 79.2a0d8d9, 2023/03/14-11:19:46
Creator Tool               : PScript5.dll Version 5.2.2
Metadata Date              : 2023:05:31 14:53:45-04:00
Format                     : application/pdf
Title                      : Complaint
Creator                   : Federal Trade Commission
Producer                  : Adobe Acrobat Pro (32-bit) 23 Paper Capture Plug-in
Document ID               : uuid:0da26833-806d-46bd-b02f-b995bdc703b8
Instance ID               : uuid:3855012c-0b9b-42e3-8819-a73274ccecd
Page Count                : 17
```

Cambiando Author y Title del archivo de Amazon.

```
kali@kali: ~/Desktop
File Actions Edit View Help
MIME Type : application/pdf
PDF Version : 1.6
Linearized : Yes
Author : Federal Trade Commission
Create Date : 2023:05:31 09:50:09-04:00
Modify Date : 2023:05:31 14:53:45-04:00
Language : en
Tagged PDF : Yes
XMP Toolkit : Adobe XMP Core 9.1-c001 79.2a0d8d9, 2023/03/14-11:19:46
Creator Tool : PScript5.dll Version 5.2.2
Metadata Date : 2023:05:31 14:53:45-04:00
Format : application/pdf
Title : Complaint
Creator : Federal Trade Commission
Producer : Adobe Acrobat Pro (32-bit) 23 Paper Capture Plug-in
Document ID : uuid:0da26833-806d-46bd-b02f-b995bdc703b8
Instance ID : uuid:3855012c-0b9b-42e3-8819-a73274ccecd
Page Count : 17

(kali㉿kali)-[~/Desktop]
└─$ exiftool -Author=Eric Amazon-Complaint-\\(Dkt.1\\).pdf
1 image files updated

(kali㉿kali)-[~/Desktop]
└─$ exiftool -Title="NewFile" Amazon-Complaint-\\(Dkt.1\\).pdf
1 image files updated
```

Resultado


```
(kali㉿kali)-[~/Desktop]
$ exiftool Amazon-Complaint-\(Dkt.1\).pdf
ExifTool Version Number      : 12.67
File Name                    : Amazon-Complaint-(Dkt.1).pdf
Directory                   : .
File Size                    : 257 kB
File Modification Date/Time   : 2023:11:09 11:37:35-05:00
File Access Date/Time        : 2023:11:09 11:37:36-05:00
File Inode Change Date/Time   : 2023:11:09 11:37:35-05:00
File Permissions              : -rw-r--r--
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.6
Linearized                   : No
Create Date                  : 2023:05:31 09:50:09-04:00
Modify Date                   : 2023:05:31 14:53:45-04:00
Language                     : en
Tagged PDF                   : Yes
XMP Toolkit                   : Image::ExifTool 12.67
Creator                      : Federal Trade Commission
Format                       : application/pdf
Title                        : NewFile
Author                       : Eric
Producer                     : Adobe Acrobat Pro (32-bit) 23 Paper Capture Plug-in
Creator Tool                  : PScrip5.dll Version 5.2.2
Metadata Date                : 2023:05:31 14:53:45-04:00
Document ID                   : uuid:0da26833-806d-46bd-b02f-b995bdc703b8
Instance ID                   : uuid:3855012c-0b9b-42e3-8819-a73274cccede
Page Count                    : 17
```

Eliminar los metadatos que he cambiado, en mi caso voy a borrar Title y Author.

```
(kali㉿kali)-[~/Desktop]
$ exiftool -Title= -Author= Amazon-Complaint-\(Dkt.1\).pdf
1 image files updated

(kali㉿kali)-[~/Desktop]
$ exiftool Amazon-Complaint-\(Dkt.1\).pdf
ExifTool Version Number      : 12.67
File Name                    : Amazon-Complaint-(Dkt.1).pdf
Directory                   : .
File Size                    : 256 kB
File Modification Date/Time   : 2023:11:09 11:43:03-05:00
File Access Date/Time        : 2023:11:09 11:43:04-05:00
File Inode Change Date/Time   : 2023:11:09 11:43:03-05:00
File Permissions              : -rw-r--r--
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.6
Linearized                   : No
Create Date                  : 2023:05:31 09:50:09-04:00
Modify Date                   : 2023:05:31 14:53:45-04:00
Language                     : en
Tagged PDF                   : Yes
XMP Toolkit                   : Image::ExifTool 12.67
Creator                      : Federal Trade Commission
Format                       : application/pdf
Producer                     : Adobe Acrobat Pro (32-bit) 23 Paper Capture Plug-in
Creator Tool                  : PScrip5.dll Version 5.2.2
Metadata Date                : 2023:05:31 14:53:45-04:00
Document ID                   : uuid:0da26833-806d-46bd-b02f-b995bdc703b8
Instance ID                   : uuid:3855012c-0b9b-42e3-8819-a73274cccede
Page Count                    : 17
```

4. Crea un nuevo proyecto en FOCA denominado “Mi proyecto en FOCA”. Analiza algún dominio que proporcione variedad de archivos. Analízalos y saca un reporte del mismo.



Foca

OPEN SOURCE

Select project

Project name

Domain website

Alternative domains

Folder where to save documents

Project date

Project notes

Project of <https://www.amazon.com/>

<https://www.amazon.com/>

C:\Users\Usuario\AppData\Local\Temp

jueves , 9 de noviembre de 2023

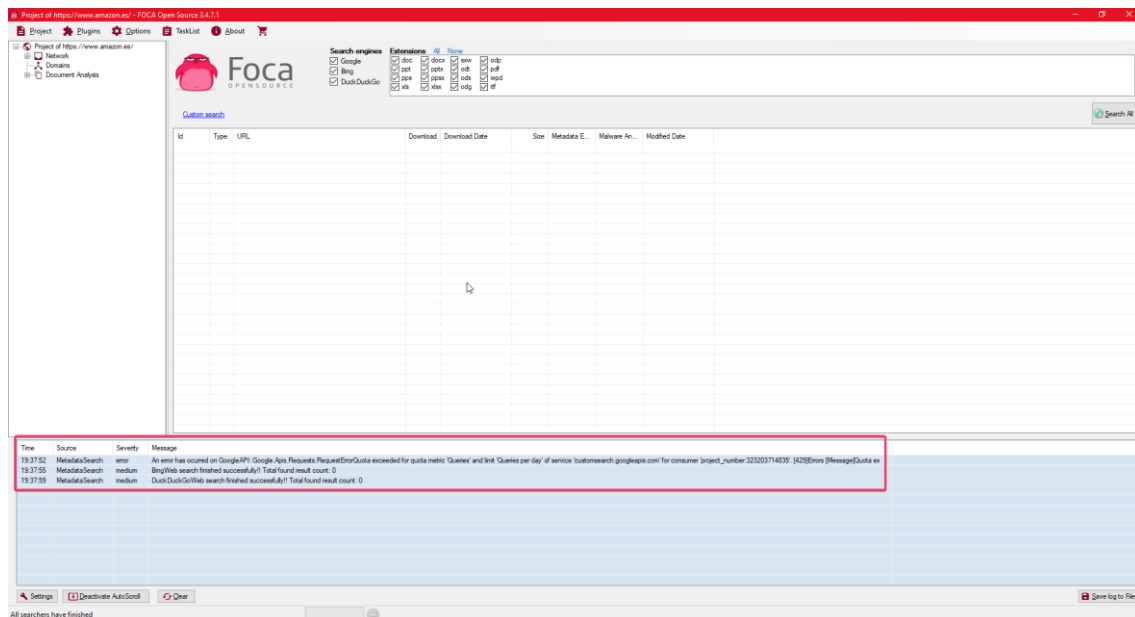
Create

Import

Cancel

[illegible]

Pensaba que habría un botón en la interfaz para hacer un informe, no lo encontré y pasé a lo siguiente. Cerré FOCA y cuando volví a esta actividad para comentarte a mano lo que estaba viendo que había encontrado, la API de Google no me dejaba hacer más búsquedas por haber hecho demasiadas por día.



Prueba de que la API de google no me dejaba hacer más consultas

ESTEGANOGRAFÍA

1. Oculta algún tipo de información en un archivo de tu elección. Prueba a extraerla.

He creado un fichero de texto en el escritorio con un mensaje, y he descargado un archivo jpg.

En el primer comando he metido el texto que había en el mensaje.txt en la imagen. Después a mano he borrado el mensaje.txt y en el segundo comando he extraído el texto de la imagen, y me ha vuelto a crear el mensaje.txt con el mismo texto que tenía.

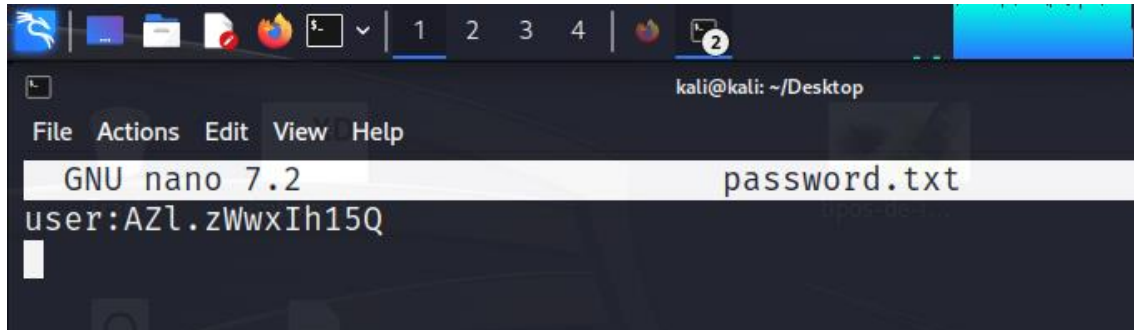
```
(kali@kali)-[~/Desktop]
$ steghide embed -ef mensaje.txt -cf tipos-de-imágenes-1280x720.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "mensaje.txt" in "tipos-de-imágenes-1280x720.jpg" ... done

(kali@kali)-[~/Desktop]
$ steghide extract -sf tipos-de-imágenes-1280x720.jpg
Enter passphrase:
the file "mensaje.txt" does already exist. overwrite ? (y/n) k
steghide: did not write to file "mensaje.txt".
```

<https://i.imgur.com/BIWB9I.gif>

2. Oculta algún tipo de información en un archivo protegido por contraseña. Realiza fuerza bruta para intentar obtener el archivo.

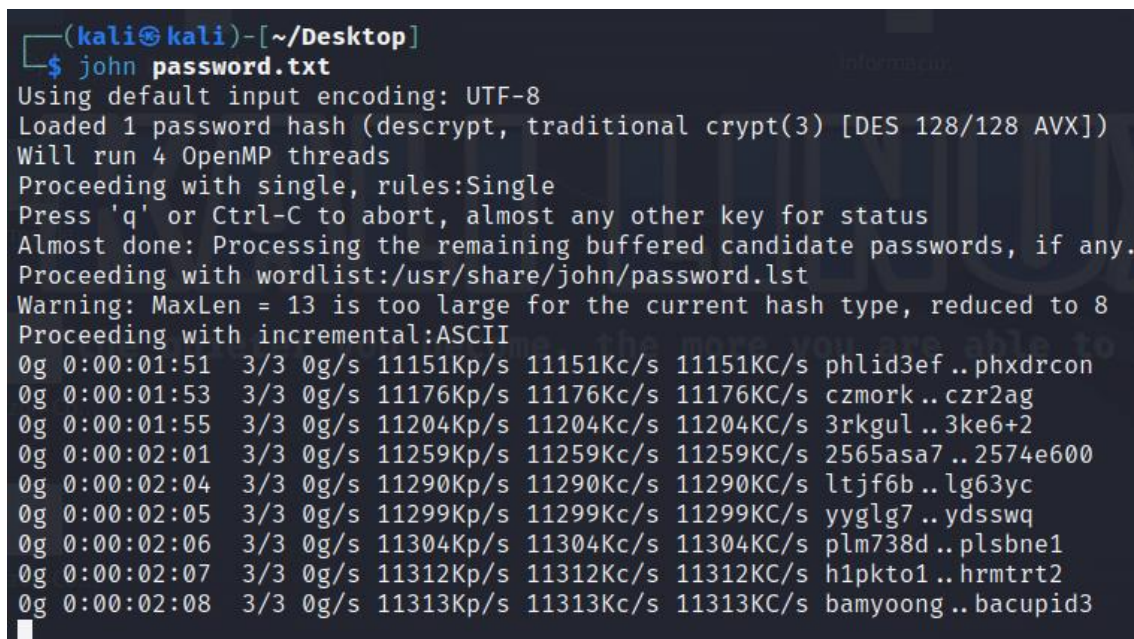
He creado el fichero password.txt y he escrito en el user:AZL.zWwxIh15Q.



```

kali@kali: ~/Desktop
File Actions Edit View Help
GNU nano 7.2 password.txt
user:AZL.zWwxIh15Q

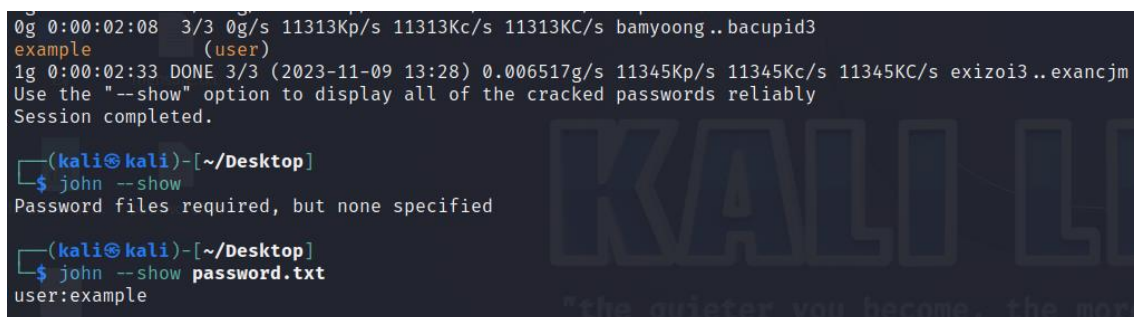
```



```

(kali@kali)-[~/Desktop]
$ john password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 AVX])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Warning: Maxlen = 13 is too large for the current hash type, reduced to 8
Proceeding with incremental:ASCII
0g 0:00:01:51 3/3 0g/s 11151Kp/s 11151Kc/s 11151KC/s phlid3ef..phxdrcon
0g 0:00:01:53 3/3 0g/s 11176Kp/s 11176Kc/s 11176KC/s czmork..czt2ag
0g 0:00:01:55 3/3 0g/s 11204Kp/s 11204Kc/s 11204KC/s 3rkgul..3ke6+2
0g 0:00:02:01 3/3 0g/s 11259Kp/s 11259Kc/s 11259KC/s 2565asa7..2574e600
0g 0:00:02:04 3/3 0g/s 11290Kp/s 11290Kc/s 11290KC/s ltjf6b..lg63yc
0g 0:00:02:05 3/3 0g/s 11299Kp/s 11299Kc/s 11299KC/s yyglg7..ydsqw
0g 0:00:02:06 3/3 0g/s 11304Kp/s 11304Kc/s 11304KC/s plm738d..plsbne1
0g 0:00:02:07 3/3 0g/s 11312Kp/s 11312Kc/s 11312KC/s h1pkto1..hrmtrt2
0g 0:00:02:08 3/3 0g/s 11313Kp/s 11313Kc/s 11313KC/s bamyoong..bacupid3

```



```

0g 0:00:02:08 3/3 0g/s 11313Kp/s 11313Kc/s 11313KC/s bamyoong..bacupid3
example (user)
1g 0:00:02:33 DONE 3/3 (2023-11-09 13:28) 0.006517g/s 11345Kp/s 11345Kc/s 11345KC/s exizoi3..exancjm
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Desktop]
$ john --show
Password files required, but none specified

(kali@kali)-[~/Desktop]
$ john --show password.txt
user:example

```

(Opcional): prueba las alternativas en desarrollo a StegCracker y realiza una comparativa de rendimiento.