Laura Bezanilla Matellán

Título:

Informe Técnico Pericial

Para:

XENON SL

Referencia:

I2F3O-2R4Z

Fecha:

22 de diciembre de 2023

Tabla de contenido

DICTAMEN PERICIAL

0 RESUMEN EJECUTIVO

Tal y como se expondrá en el presente informe, en opinión de este perito, el análisis del dispositivo móvil del acusado ha arrojado las siguientes conclusiones:

Una vez analizado el móvil Android, este perito estima que Javier García ha hecho uso de técnicas de esteganografía digital para poder ocultar un fichero de texto plano en una imagen sin alterar la apariencia de esta.

A juicio de este perito lo primero que ha realizado el acusado es apuntar la contraseña de la aplicación de esteganografía que ha utilizado en un documento que posteriormente ha protegido con una contraseña de tres dígitos numéricos.

Posteriormente, tras haber realizado un análisis minucioso del dispositivo móvil del acusado, este perito estima que existe una imagen en formato JPG que oculta un mensaje en su interior.

En conclusión, tal y como se expondrá en el presente informe, en opinión de este perito, el análisis realizado indica que se han encontrado las evidencias necesarias sobre la ocultación del fichero en una imagen por parte del acusado Javier García a través de una herramienta de esteganografía llamada *Steganofile*.

1 INTRODUCCIÓN

1.1 Sobre el Objeto del Peritaje

A requerimiento de XENON S.L. se procede a la revisión de un caso de esteganografía digital. En dicho caso se demanda a Javier García por la ocultación de un fichero en texto plano en una fotografía.

Considerando los hechos y circunstancias anteriores, el Perito autor del presente informe técnico, de conformidad con lo dispuesto por el artículo 335.2 de la *Ley de Enjuiciamiento Civil*, quiere hacer las siguientes manifestaciones:

- **El presente dictamen lo emite bajo promesa de decir la verdad.**
- **Ha actuado con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes.**

El perito manifiesta su total imparcialidad y la **no concurrencia de ninguna de las circunstancias** por las que poder ser objeto de tachas, recogidas en el artículo 343 de la Ley de Enjuiciamiento Civil:

- Ser cónyuge o pariente por consanguinidad o afinidad, dentro del cuarto grado civil de una de las partes o de sus abogados o procuradores.
- Tener interés directo o indirecto en el asunto o en otro semejante.
- Estar o haber estado en situación de dependencia o de comunidad o contraposición de intereses con alguna de las partes o con sus abogados o procuradores.
- Amistad íntima o enemistad con cualquiera de las partes o sus procuradores o abogados.
- Cualquier otra circunstancia, debidamente acreditada, que les haga desmerecer en el concepto profesional.

1.2 Sobre el Perito

La Colegiado nº 11 del *Ilustre Colegio Profesional de Ingenieros en Informática de Madrid* (https://cpiicm.es) es **Licenciada e Ingeniera / Máster en Informática** por la Universidad Autónoma de Madrid.

Profesionalmente, desempeña su actividad principal como **consultor en una reconocida empresa de seguridad informática, donde se especializa en el análisis de dispositivos móviles Android.**

Ha recibido formación como perito por parte del **Colegio Profesional de Ingenieros en Informática de Madrid y por parte de Jaime Zurro**, además de cursar un máster en informática forense impartido por la Universidad Autónoma de Madrid. Por último, ha llevado a cabo numerosos peritajes similares al del presente documento en el ámbito de análisis de dispositivos Android y casos de esteganografía.

2 CONSIDERACIONES GENERALES

2.1 Sobre la esteganografía digital

La esteganografía digital es considerada un arte que está en constante evolución capaz de adaptarse a las nuevas tecnologías que se van desarrollando. Este tipo de arte está muy relacionado con la rama de la criptografía.

La esteganografía consiste en la aplicación de diferentes técnicas que permiten la ocultación de información dentro de un mensaje de forma que no sea evidente a simple vista que existen datos ocultos. Este método de ocultación es comúnmente utilizado en archivos de imágenes, audio o incluso en documentos de texto.

En conclusión, la esteganografía se basa en incorporar datos a un archivo sin tener que cifrar dicha información. Por ejemplo, modificar ciertos pixeles de una imagen para poder ocultar información sin modificar la apariencia del archivo original.

2.2 Sobre el uso de contraseñas en documentos

Actualmente, la protección de documentos con una contraseña proporciona una capa adicional de protección contra accesos no autorizados. El uso de este tipo de contraseñas puede ayudar a proteger información confidencial de un archivo. Por ello, hacer uso de ellas es importante en lugares donde la confidencialidad de los datos es muy importante, como por ejemplo las empresas privadas o las organizaciones gubernamentales.

Por otro lado, la implementación de contraseñas sólidas junto con la puesta en marcha de buenas prácticas en la gestión de contraseñas puede mejorar considerablemente la integridad de los datos almacenados en los documentos.

En este informe pericial, se tratará el uso de contraseñas en un documento Word con la versión 2016 para evitar dentro de lo posible que cualquier persona no autorizada pueda acceder o modificar el contenido del documento.

2.3 Sobre los ataques para la obtención de contraseñas de los documentos

Hoy en día con el avance de la tecnología existen diferentes métodos para poder obtener la contraseña de un sistema. Uno de los más sencillos y, probablemente el más utilizado cuando las contraseñas tienen una longitud corta, es el ataque por fuerza bruta.

Para llevar a cabo este tipo de ataque es necesario hacer pruebas con todas las posibles combinaciones que puedan existir aprovechando la vulnerabilidad de las contraseñas débiles.

Sin embargo, para reducir el tiempo necesario para poder obtener la contraseña utilizando este método existe la posibilidad de realizar el ataque de manera dirigida. Es decir, cuando se sabe la longitud de la contraseña así como el tipo de sus caracteres, si son letras o números, es posible indicárselo a la herramienta para que se reduzca de manera considerable el número de combinaciones que tiene que probar.

Por todo ello, para poder evitar que estos ataques tengan éxito es necesario utilizar contraseñas robustas que estén formadas por diferentes tipos de caracteres desde mayúsculas, minúsculas y dígitos numéricos hasta caracteres especiales.

2.4 Sobre las funciones de resumen HASH

Los hashes, también llamadas funciones resumen, son algoritmos que, a partir de una entrada de cualquier tamaño, como por ejemplo una contraseña o un archivo son capaces de transformarlo en una cadena de salida alfanumérica de longitud fija, lo que se conoce como hash.

Si se produce cualquier cambio pequeño en los datos originales, el algoritmo generará una salida completamente diferente. Por ello, hacer un buen uso de las funciones hash es muy importantes para poder garantizar tanto la integridad como la seguridad de los datos en un peritaje forense.

En este peritaje en concreto se utilizarán las funciones hash SHA-1.

2.5 Sobre la conexión de dispositivos Xiaomi

Todos los dispositivos móviles de Xiaomi permiten realizar una navegación por las diferentes carpetas del dispositivo una vez que se ha conectado a un ordenador. Es importante destacar que esta navegación se realizará en modo solo lectura utilizando la herramienta USB Write Protector para evitar cualquier tipo de manipulación de la evidencia.

A través de esa conexión en modo solo lectura se procederá a extraer la imagen que se está investigando en la carpeta del dispositivo con nombre "*shared/0/Download* ".

Finalmente, todos los ficheros, una vez creado su código HASH, se almacenan en un dispositivo USB con número de serie "X1Y2Z3A4B5C6D7E8F9G0H1I2" que se presentará como evidencia en este peritaje.

2.6 Sobre la herramienta USB Write Protector

USB Write Protector es una herramienta gratuita que permite activar la protección contra escrituras de todos los dispositivos de almacenamiento USB que se conecten a un ordenador.

Esta herramienta se caracteriza por su facilidad de uso ya que solo es necesario ejecutar el programa y elegir entre activar o desactivar esta protección. Al utilizar esta herramienta, se estaría evitando la escritura de datos en el dispositivo. De esta forma se garantiza mantener la integridad de la evidencia.

2.7 Sobre la herramienta online LostMyPass

LostMyPass es una herramienta online que te permite recuperar contraseñas de documentos PDF y Microsoft Office, así como archivos comprimidos de tipo RAR y Zip.

Esta herramienta ofrece un servicio rápido y fácil de usar ya que no es necesario instalar ningún tipo de software. Además, gracias al diseño limpio de su interfaz y su facilidad de uso la convierte en una herramienta eficaz en caso de que no se quiera pagar para poder utilizar este tipo de servicios.

Su funcionamiento para poder obtener la contraseña es muy simple, solo hay que arrastrar o cargar el documento que esté protegido con una contraseña para posteriormente elegir el tipo de ataque que se quiere realizar para conseguir la contraseña. Una vez se ha configurado la información solo hay que esperar unos minutos a que sus servidores realicen las operaciones necesarias para poder conseguir el objetivo.

Finalmente, cuando la herramienta tenga éxito se mostrará la contraseña del documento lo que permitirá poder abrirlo y ver su contenido

Se debe tener en cuenta que este servicio gratuito solo está disponible para la recuperación de contraseñas débiles como es el caso que se está investigando en este informe pericial.

2.8 Sobre la herramienta Andriller

Andriller es una herramienta de análisis forense automático de código abierto que permite la extracción de información de un dispositivo móvil Android, donde no se tienen permisos de super usuario, utilizando diferentes técnicas forenses avanzadas, entre las que se incluye el acceso a la memoria RAM, así como la extracción de datos de las aplicaciones instaladas en el sistema.

El uso de esta herramienta es bastante sencillo. Lo primero que hay que hacer es conectar el móvil Android al ordenador mediante un cable USB. Una vez conectado el dispositivo se seleccionará en la herramienta para posteriormente poder elegir el tipo de análisis que se quiere efectuar sobre dicho dispositivo.

Además, esta herramienta ofrece la posibilidad de generar reportes para poder tener un informe detallado del análisis forense que se ha llevado a cabo.

3 CONSIDERACIONES ESPECÍFICAS

3.1 Sobre la activación del modo solo lectura del USB

Para este peritaje informático lo primero que se ha hecho es ejecutar la herramienta USB Write Protector descrita en el apartado 2.6 para poder habilitar el modo lectura en el sistema.

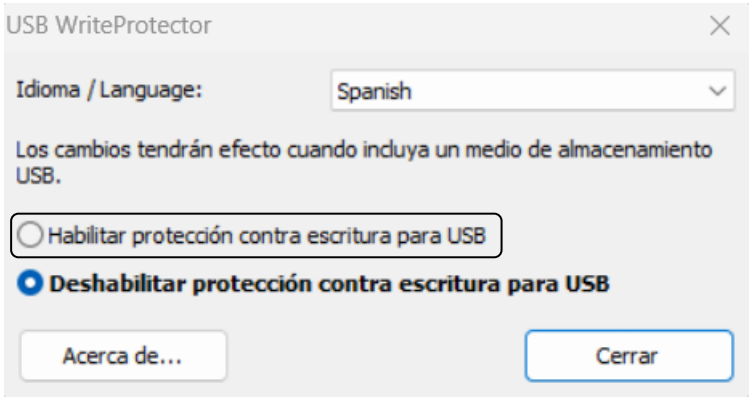

Figura 1. Activación del modo lectura en la herramienta

Por otro lado, para estar totalmente seguros de que no se va a alterar la evidencia se va a proceder a activar la protección contra escritura de un USB que ofrece el sistema operativo Windows.

Para ello, el primer paso es ejecutar la aplicación "Ejecutar" propia de Windows para poder abrir el programa "Regedit" como se muestra a continuación.

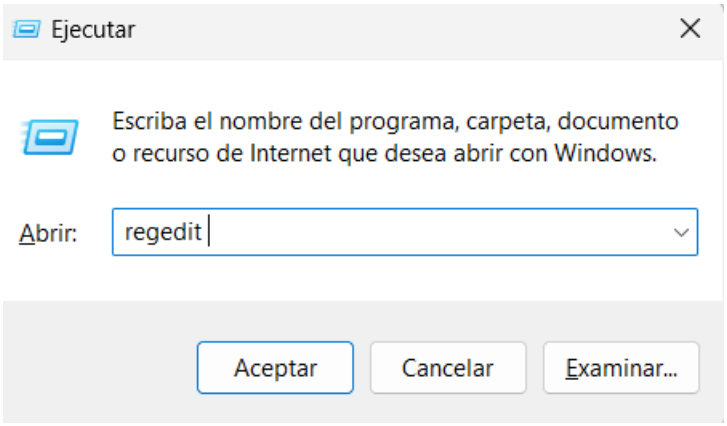

Figura 2. Abrir el programa Ejecutar

El siguiente paso es pulsar el botón de "Aceptar" lo que causará que Windows pregunte si se quiere permitir que esta aplicación haga cambios en el equipo, a lo que habrá que pulsar que "Sí".

A continuación, se abrirá el editor de registro donde habrá que navegar hasta llegar a la sección de "*StorageDevicePolicies*". Para ello, habrá que seguir esta ruta:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies
```

Una vez dentro de esa carpeta se hará doble click sobre la variable "WriteProtect" que es el valor que controla la escritura en los dispositivos USB. Esta acción abrirá la ventana de la *Figura 3* para poder modificar el valor.

Por último, se cambiará el valor cero por un uno para poder habilitar esta protección contra la escritura.

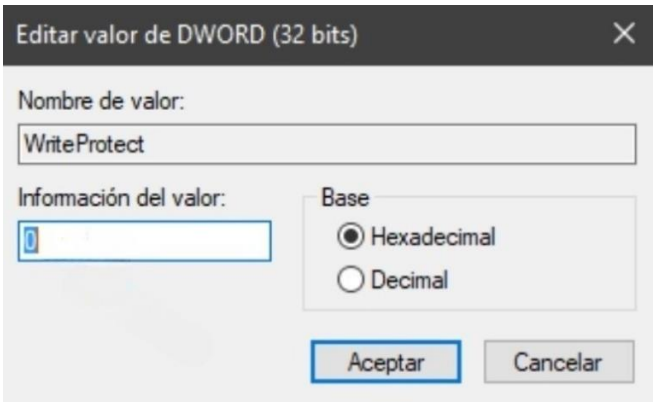

Figura 3. Editar el valor de la variable WriteProtect

3.2 Sobre la extracción de los datos de un dispositivo Android

Después de asegurar que el modo lectura para los USB está habilitado, el siguiente paso es utilizar la herramienta Andriller en la versión 3.6.3 para proceder con la extracción del sistema de archivos del almacenamiento compartido del dispositivo móvil Android.

Utilizando esta herramienta para poder obtener una copia lógica de los ficheros que se necesitan en este peritaje garantiza que no se produzca ningún tipo de modificación sobre ellos. Además, permite al perito trabajar sobre una copia en vez de sobre los datos originales del dispositivo.

A continuación, se muestra una imagen de la apariencia del programa Andriller. En primer lugar se configura el directorio donde se van a almacenar los reportes generados por esta herramienta.

Después se elige la opción de "extracción a través de USB" para poder comprobar si detecta automáticamente el dispositivo Android. Si es así mostrará el número de serie del dispositivo como se muestra en la *Figura 4*.

Finalmente, se elige la opción de "extraer el almacenamiento compartido" y se pulsa el botón de "Extract".

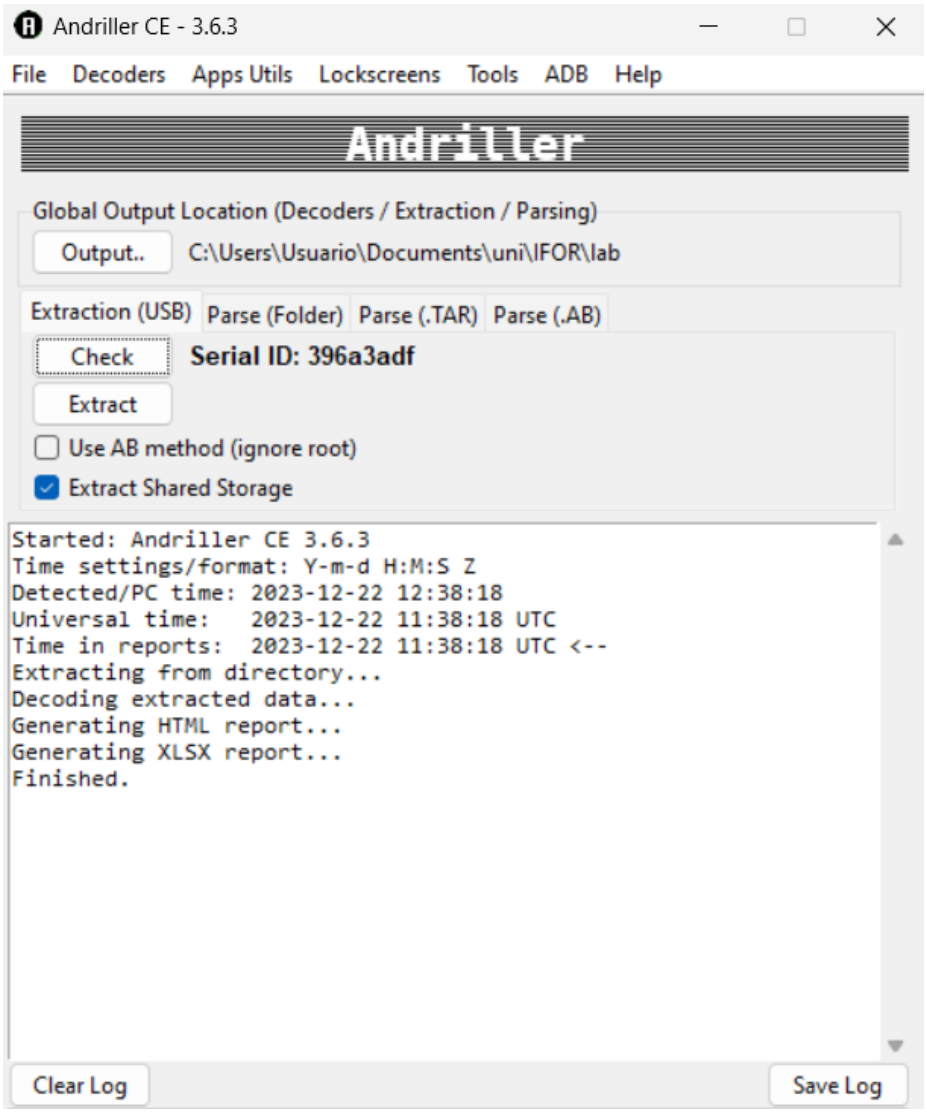

Figura 4. Configuración de Andriller

En la *Figura 5* se muestra la prueba de como la extracción ha tenido éxito y ha finalizado correctamente generando un reporte con el formato HTML que se analizará más adelante.

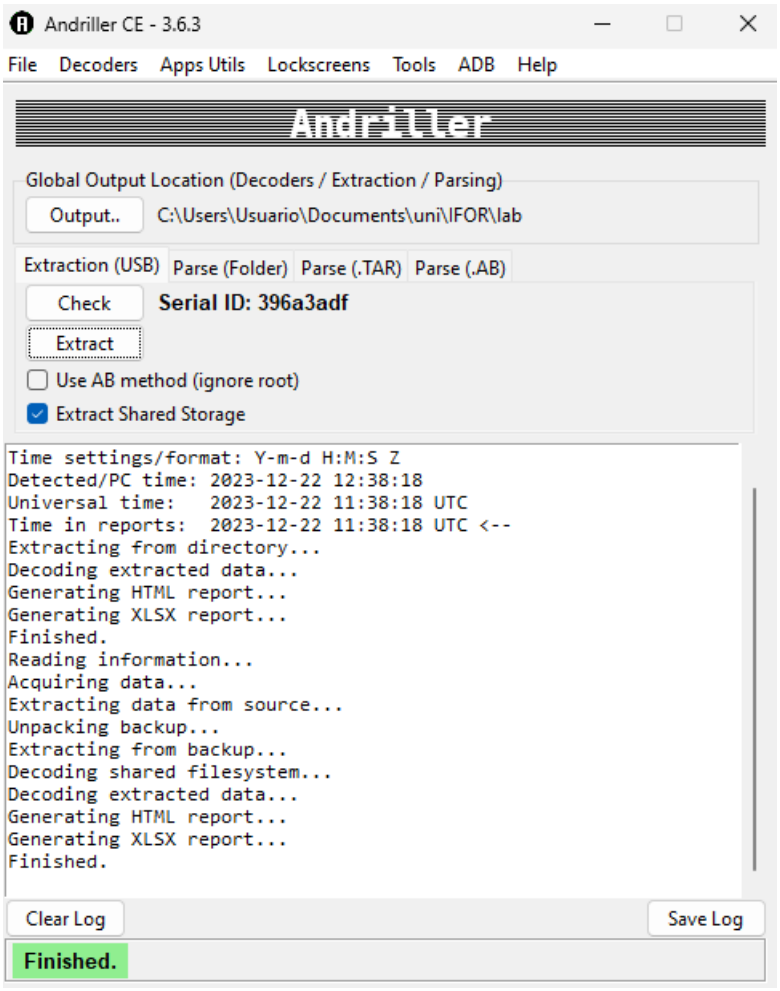

Figura 5. Extracción de datos finalizada correctamente

Esta herramienta cuando finaliza el proceso de extracción genera un reporte sobre los datos que ha obtenido en el proceso. Este reporte muestra distinta información como por ejemplo la hora local en la que se ha realizado, así como la información sobre las diferentes cuentas que tiene configuradas el dispositivo.

A continuación, se muestra dicho reporte:

This report was generated using Andriller CE # (This field is editable in Preferences)

[Andriller Report]

Type	Data
Serial	396a3adf
Status	device
Permisson	shell
Wifi Mac	ae:3d:1d:65:0c:24
Local_Time	2023-12-22 12:53:22 Hora est&#65533;ndar romance
Device_Time	2023-12-22 12:53:22 CET
Accounts	• com.google: laurabezm***gmail.com • com.google: laurabezma***gmail.com • com.xiaomi: 1840***725 • org.telegram.messenger: 855***686 • com.twitter.android.auth.login: Laur***M_11 • com.whatsapp: Wha***pp • com.zhiliaoapp.musically: Ti***k • com.pinterest.accounttransfer.type: Pin***est
Application	Shared Storage (5697)

 # andriller.com # (This field is editable in Preferences)

Figura 6. Reporte generado por Andriller en formato HTML

Si se pulsa sobre el almacenamiento compartido, es decir sobre el enlace con nombre "Shared Storage" se obtiene una tabla con 5697 elementos. Sin embargo, al ser un informe generado en HTML se puede buscar el término "*Download*" ya que se tiene la sospecha de que la imagen que se está buscando se ha transferido al dispositivo a través de un correo electrónico.

En efecto, como se puede observar en la *Figura 7,* dentro de la carpeta de descargas existe una imagen que por el nombre parece sospechosa por lo que se procederá a analizarla detalladamente más adelante.

Índice de C:\Users\Usuario\Documents\uni\IFOR

[directorio principal]

Nombre	Tamaño	Fecha de modificación
Browser/		2/4/22, 21:09:10
downloaded_apex/		17/7/21, 15:42:34
downloaded_rom/		21/12/23, 21:45:52
MGC_CRASH_LOG/		22/12/23, 13:08:19
API.php	23.2 kB	3/11/21, 10:03:01
certificado_vacunacion_covid_CYL2548333266.pdf	166 kB	1/12/21, 22:32:37
CV.pdf	108 kB	26/10/23, 23:38:50
Documento.pdf	377 kB	31/10/23, 22:30:47
eduroam-android_recent-UdV-Eduroam.eap-config	23.2 kB	25/10/21, 11:35:23
esteganografia.jpg	1.9 MB	21/12/23, 21:29:15
HorGrado_PS_1C_2023_24.pdf	1.2 MB	7/9/23, 11:20:20
iPhone-Alarm-Original.mp3	519 kB	24/9/23, 0:25:22

Figura 7. Evidencia de la imagen encontrada en el dispositivo

3.3 Sobre obtener la contraseña del documento Word

Para la realización de este peritaje se ha entregado un documento Word protegido con una contraseña que se sabe que tiene carácter numérico y una longitud de tres dígitos.

Debido a la información que se tiene disponible sobre el tipo de contraseña que tiene el documento, se va a proceder a obtener dicha contraseña a través de un ataque de fuerza bruta utilizando la herramienta **LostMyPass** detallada en el apartado 2.7.

Esta herramienta tiene la siguiente apariencia:

Figura 8. Herramienta LostMyPass

Para poder obtener la contraseña, arrastramos dicho documento Word hasta ponerlo en esa casilla. Una vez el archivo esté cargado, la página empezará a realizar las operaciones necesarias.

Unos pocos segundos después se ha obtenido de forma correcta la contraseña del documento como se muestra a continuación:

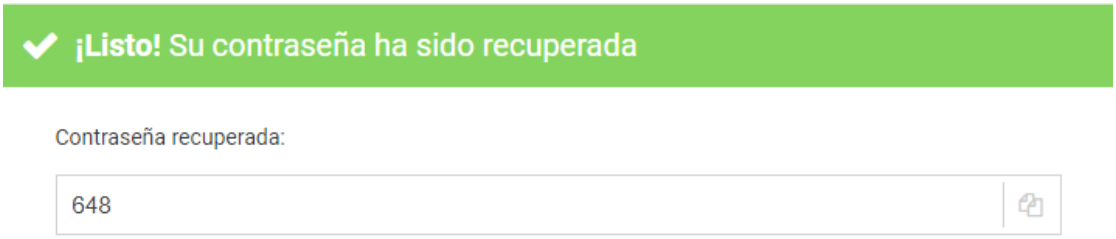

Figura 9. Obtención exitosa de la contraseña del documento

Como en este punto del peritaje ya se ha obtenido la contraseña del documento y además se tiene una imagen sospechosa, se va a proceder a abrir dicho documento para poder analizar qué tipo de información secreta contiene.

Al abrir el documento aparece una ventana para poder introducir la contraseña como se muestra en la *Figura 10*:

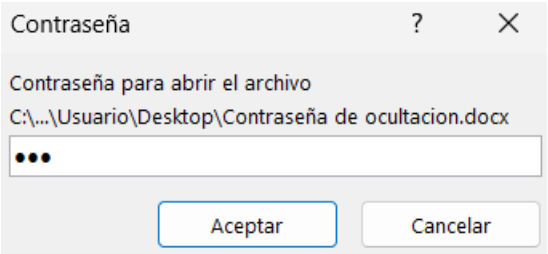

Figura 10. Introducción de la contraseña del documento

Cuando se pulsa "Aceptar" se puede comprobar que el contenido del documento es la siguiente frase:

La contraseña de ocultación es: 7777

Finalmente, si se analiza con detalle el escenario que se está investigando se puede llegar a la conclusión de que el acusado Javier García ha ocultado información en la imagen extraída haciendo uso de un programa que necesita contraseña.

3.4 Sobre obtener el mensaje oculto en la imagen

Después de extraer de forma cuidadosa la imagen del dispositivo Android y obtener la contraseña del documento Word, el siguiente paso en el peritaje forense sería averiguar qué tipo de información ha intentado ocultar en la imagen el acusado.

Para ello, se ha realizado una investigación de las herramientas [1] de esteganografía más populares en el mercado. Después de este proceso de prueba de todos los programas existentes en la página se puede concluir que el acusado ha utilizado la herramienta llamada *Steganofile*.

Esta herramienta permite ocultar un archivo secreto dentro de otro archivo. Como se puede observar en la *Figura 11*, su interfaz de usuario tiene dos botones que permiten codificar o decodificar archivos. Además también tiene integrada la opción de poder eliminar el archivo original después de la codificación.

Figura 11. Interfaz de la aplicación Steganofile

Para este peritaje en concreto se necesita la opción decodificar. El siguiente paso es configurar la imagen que se quiere decodificar así como la contraseña necesaria para ello. El último paso es establecer la carpeta donde se van a depositar los archivos que estaban ocultos como se observa en la *Figura 12*.

Cuando la herramienta ha terminado de analizar la imagen sospechosa aparecerá una ventana emergente con el resultado de los ficheros secretos que se han extraído de la imagen.

En este caso concreto el resultado que arroja la herramienta es que el acusado ha ocultado en la imagen un fichero de texto plano que se llama "urls de interés.txt" como se muestra en la *Figura 13*.

[1] *Se han analizado las herramientas que aparecen en esta página web:* https://listoffreeware.com/list-of-best-free-steganography-software-for-windows/

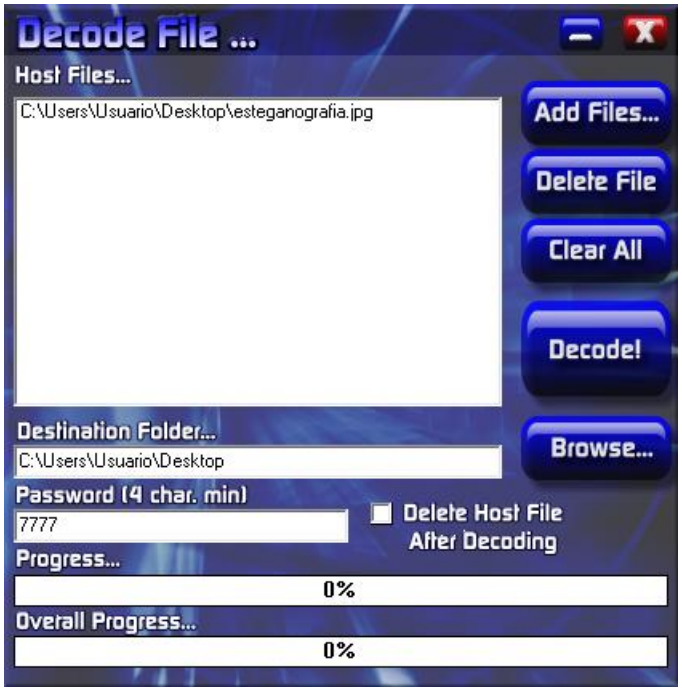

Figura 12. Configuración del funcionamiento de la herramienta

Figura 13. Fichero oculto en la imagen

Finalmente, se procede a abrir dicho documento para poder concluir que tipo de datos ha ocultado el acusado en la imagen.

Al abrir ese fichero se muestra que contiene únicamente la siguiente dirección web:

https://www.genbeta.com/windows/asi-puedes-recuperar-archivos-borrados-windows-10-nueva-app-gratuita-microsoft

4 CONCLUSIONES

En opinión de este perito, después de haber analizado el dispositivo móvil del acusado, puede concluir que Javier García ha ocultado un fichero secreto en una imagen utilizando técnicas de esteganografía digital.

Además, este perito puede afirmar que la información que se estaba tratando de ocultar es la dirección de la siguiente página web:

https://www.genbeta.com/windows/asi-puedes-recuperar-archivos-borrados-windows-10-nueva-app-gratuita-microsoft

Lo que hago constar como perito en este dictamen, salvo mejor opinión a la que me someto, para lo cual, pondré a disposición de quien lo solicite, todos los medios utilizados para llegar a las conclusiones a las que he llegado.

Emito por tanto este dictamen extendido en 21 folios, según mi leal saber y entender, prometiendo que en el momento de emitirlo, he dicho la verdad y he actuado con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes.

Laura Bezanilla Matellán y Firma del perito

En Valladolid a 22 de diciembre de 2023.

5 SOBRE LA METODOLOGÍA EMPLEADA EN LA ELABORACIÓN DEL PRESENTE INFORME PERICIAL

Para la elaboración de este dictamen, la metodología empleada ha sido la siguiente:

1. Revisión de la documentación entregada por XENON SL.
2. Revisión de los documentos aportados por el juez.
3. Realización de la extracción segura del almacenamiento interno del dispositivo, con el fin de preservar la cadena de custodia.
4. Revisión del software utilizado para ocultar el mensaje en la imagen.
5. Estudio y documentación de las evidencias encontradas sobre las pruebas recibidas.
6. Redacción del presente informe.

6 BIBLIOGRAFÍA Y REFERENCIAS A CONSULTAR

Para la elaboración de este dictamen, este perito se ha basado además de en sus conocimientos, en una serie de referencias bibliográficas sobre Ingeniería Informática entre las que se encuentran:

1. Recursos de la asignatura Informática Forense. Campus Virtual
2. Apuntes de la asignatura Informática Forense. Campus Virtual

3. Herramienta LostMyPass: https://www.lostmypass.com/es/file-types/ms-word/
4. Herramienta Andriller: https://github.com/den4uk/andriller
5. Herramienta Steganofile: https://www.softpedia.com/get/Security/Encrypting/Steganofile.shtml

EVIDENCIAS

Para la realización de este informe se han utilizado un conjunto de evidencias que se detallan a continuación:

Se adjuntan como evidencias los archivos implicados en el caso, extraídos en una memoria USB con número de serie: X1Y2Z3A4B5C6D7E8F9G0H1I2, los cuales están referenciados a continuación:

1. Fichero en formato Word que contiene la contraseña utilizada en la herramienta Steganofile : <D:\Evidencias_LauraBezanilla\Contraseña de ocultacion.docx >

SHA-1: 795ADB924C8420F59A20EBFDF81207D5C209E9FC

2. Dispositivo móvil Android incautado al acusado, en el que se encuentra la imagen con el mensaje oculto.

3. Fichero en formato JPG con la imagen que tiene el mensaje oculto: < D:\Evidencias_LauraBezanilla\ esteganografia.jpg >

SHA-1: C3F725F9E781E6123F5B3405B13DA90D10318547

4. Fichero en texto plano el cual ha sido ocultado en la imagen: <D:\Evidencias_LauraBezanilla\ urls de interes.txt>

SHA-1: FCB568907BD05F3B260AAE73EAAF1D8C124A3E49

5. Reporte en formato HTML generado por la herramienta Andriller: <D:\Evidencias_LauraBezanilla\ REPORT.html>

SHA-1: A8D1A9C55983F07B8465272EF1EFA69FF6023FCC