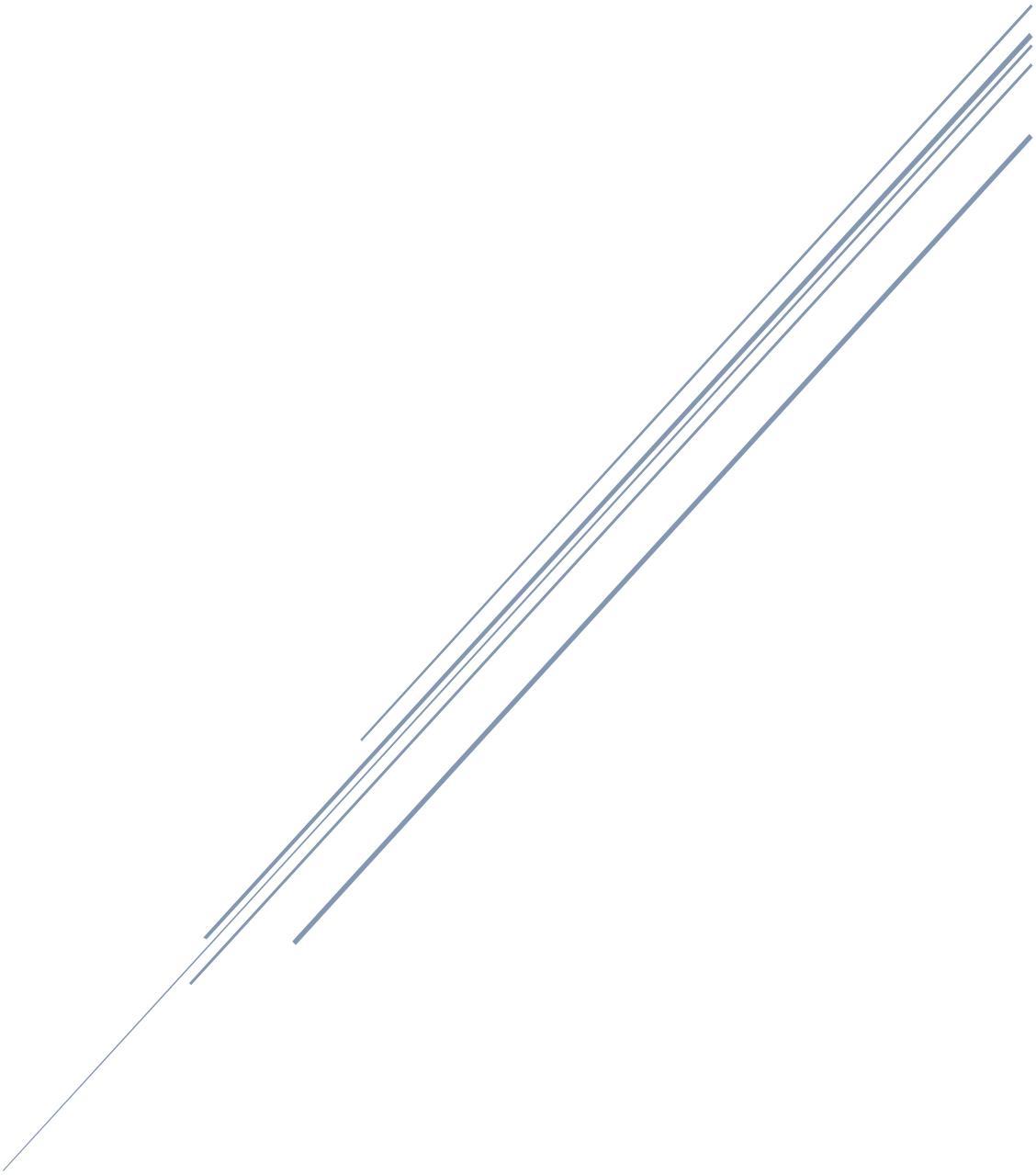
Sierra de Guara
instituto de educación secundaria

INFORME ANÁLISIS FORENSE

BORRADO DE INFROMACIÓN



ID Expediente: EX2765EV
Eduardo Villacampa Escartín

1. IDENTIFICACIÓN

1.1. Título

Título del informe: **Informe de análisis forense – Borrado de información**

1.2. Código único

Código de identificación del caso: **2023-EVE-BOR-1000**

1.3. Identificación del perito + juramento/promesa

Nombre	***Apellidos***	***Contacto***
Eduardo	Villacampa Escartín	678123456 eduardovillacampa@perito.com Plaza Navarra, Nº.2, 2ª, 22002 (Huesca)

N.º de colegiado
27453
Titulación académica
Técnico Superior en Sistemas de Telecomunicaciones e Informáticos Especialista en Ciberseguridad en entornos de la Tecnología de la Información Profesional titulado en la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos (ANTPJI)

JURAMENTO

El perito declara:

Yo, **D. Eduardo Villacampa Escartín**, con DNI 12345678-Z, Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, con titulación académica de Especialista en Ciberseguridad en entornos de las Tecnologías de la Información, colegiado en la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos (ANTPJI, con Nº de colegiado **27453**, al emitir el presente informe prometo decir la verdad, actuar 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. Declaro también el conocimiento de las sanciones penales en las que podría incurrir si incumplo mi deber como perito.

1.4. Destinatario

El destinatario del informe de análisis forense con identificador **EX2765EV**, correspondiente al caso **2023-EVE-BOR-1000** es **el Juzgado de Primera Instancia e Instrucción Nº 1 de Huesca.**

Dirección	C/ Calatayud, s/n
Código Postal	22005
Municipio - Provincia	Huesca – Huesca
Teléfono/s	974 29 01 14 – 974 29 01 13
E-mail	mixto1huesca@justicia.aragon.es

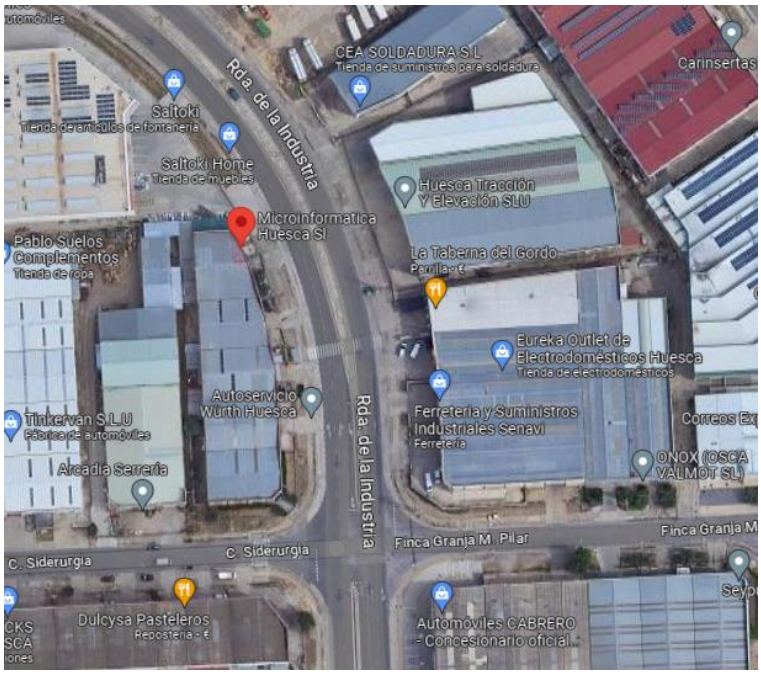
1.5. Solicitante

El solicitante del informe de análisis forense es **D. Jorge Gutiérrez Palo**, con DNI **98765432-A,** directivo de la empresa **Microinformática Huesca S.L** con CIF **B22220545,** personándose D. Jorge Gutiérrez Palo como solicitante en nombre de la empresa.

1.6. Emplazamiento geográfico

El día 21 de marzo de 2023, se realizó un clonado de disco duro y un volcado de memoria RAM de un ordenador de escritorio situado en la empresa **Microinformática Huesca S.L, localizada en Polígono Industrial Sepes, Parcela 59, Ronda de la Industria, s/n, 22006 Huesca.**

Coordenadas GPS: 42.1465855,-0.3889547



Posteriormente, se analizó la imagen del disco y el volcado de memoria en el lugar de trabajo del perito informático, localizado en **Plaza Navarra, Nº.2, 2ª, 22002 (Huesca).**

Coordenadas GPS: 42.1361342,-0.4082906.

1.7. Letrado y/o procurador

La letrado **Dª Noemi Ainsa Montañes,** colegiado **N.º 637** en el **Ilustre Colegio de Abogados de Huesca**, solicita la realización de la pericial.

Datos de colegiación	
Nombre	NOEMI AINSA MONTAÑES
Colegio	HUESCA
Alta Colegiación	31/12/1995
N.º Colegiado	637
Datos de contacto	
Dirección profesional	Calle Serrablo, Nº71, 22600, Sabiñánigo (Huesca)
Teléfono	974480961
Fax	974480968

1.8. Declaración de tachas

Yo, **D. Eduardo Villacampa Escartín,** en base al Art.343 de la Ley de Enjuiciamiento Civil, declaro a la fecha de elaboración del informe, no tener conocimiento de estar en ninguna causa de tachas, ni tengo parentesco ni relación con el demandado.

2. ÍNDICE

-

-

-

3. CUERPO

3.1. Objeto

El objetivo del análisis forense realizado es **demostrar que se ha borrado un documento del ordenador de un directivo** de la empresa Microinformática Huesca S.L., D. Jorge Gutiérrez Palo.

3.2. Alcance

El alcance del análisis forense ha sido acordado por parte del representante de la empresa Microinformática Huesca S.L., D. Jorge Gutiérrez Palo y el perito forense D. Eduardo Villacampa Escartín.

Se ha realizado un análisis forense al ordenador de D. Jorge Gutiérrez Palo, presente en las instalaciones de Microinformática Huesca S.L., con el objetivo de certificar si se ha borrado el archivo llamado ***"Redalyc_El_libro_digital_nuevos_formatos_de_lectura.pdf".***

Para ello, el día 21 de marzo de 2023, se realizó un clonado de disco y un volcado de memoria RAM de un ordenador de escritorio situado en la empresa **Microinformática Huesca S.L, localizada en Polígono Industrial Sepes, Parcela 59, Ronda de la Industria, s/n, 22006 Huesca.**

Posteriormente, se analizó la imagen del disco y el volcado de memoria en el lugar de trabajo del perito informático, localizado en **Plaza Navarra, Nº.2, 2ª, 22002 (Huesca).**

A su vez, se realizó una entrevista entre el perito D. Eduardo Villacampa Escartín y D. Jorge Gutiérrez Palo.

El objetivo de este análisis es responder a las siguientes preguntas:

- ¿El archivo *"Redalyc_El_libro_digital_nuevos_formatos_de_lectura.pdf"* fue eliminado del ordenador de D. Jorge Gutiérrez Palo*?*
- ¿Quién borró el archivo?
- ¿Cuándo se borró el archivo?
- ¿El archivo fue borrado intencionadamente?
- ¿Cómo es posible recuperar el archivo si se ha borrado?

Estas preguntas serán respondidas en al apartado '*Conclusiones'.*

3.3. Antecedentes

D. Jorge Gutiérrez Palo conoce los servicios del perito D. Eduardo Villacampa Escartín, a través de su abogada Dª Noemi Ainsa Montañes. Decide contratar sus servicios profesionales de peritaje y se firma el correspondiente acuerdo de confidencialidad, que se incluye en los anexos del presente informe.

Es por ello que el perito D. Eduardo Villacampa Escartín acude a las instalaciones de la empresa para realizar un volcado de memoria y un clonado del disco duro del ordenador afectado, cuyo número de serie es PF1LD9PP, con el objetivo de analizarlos y descubrir si ese archivo fue eliminado.

D. Jorge Gutiérrez Palo fue entrevistado por el perito D. Eduardo Villacampa Escartín en presencia de su abogada, Dª Noemi Ainsa Montañes, colegiada N.º 637 en el Ilustre Colegio de Abogados de Huesca, con el objetivo de obtener información que pudiera ayudar al caso.

D. Jorge Gutiérrez Palo aseguró no haber borrado el archivo, ni haber notado ningún comportamiento extraño en su ordenador.

3.4. Consideraciones preliminares

En un sistema informático, al borrar un archivo, este permanece un tiempo en el disco de almacenamiento, aunque haya sido eliminado y no pueda ser visible de una manera normal. Existen herramientas que permiten recuperar archivos que han sido borrados anteriormente, como se explicará posteriormente en este informe.

Para entender el informe es necesario la definición de los siguientes conceptos:

- **Volcado de memoria:** acción que se realiza para obtener el estado de la memoria RAM de un equipo en un momento en concreto, con el objetivo de analizarla mediante la utilización de diferentes herramientas.
- **Clonado de disco:** proceso por el cual se obtiene una 'copia' de un disco de almacenamiento concreto, con el objetivo de poder analizar la información que contiene en otro emplazamiento.
-

3.5. Documentos de referencia

3.6. Terminología y abreviaturas

- **Volcado de memoria:** acción que se realiza para obtener el estado de la memoria RAM de un equipo en un momento en concreto, con el objetivo de analizarla mediante la utilización de diferentes herramientas.
- **Clonado de disco:** proceso por el cual se obtiene una 'copia' de un disco de almacenamiento concreto, con el objetivo de poder analizar la información que contiene en otro emplazamiento.
- **Memoria RAM:** las siglas RAM significan memoria de acceso aleatorio. Esta memoria es un banco de memoria temporal del ordenador que almacena los datos que necesita recuperar rápidamente.
- **Disco de almacenamiento:** dispositivo en el que se almacenan los datos de un ordenador.
- **Archivo (informática):** un archivo es cualquier documento que almacenes en un ordenador (música, vídeos, fotos, documentos de texto, etc).
- **Software:** programa informático.
- **Partición:** nombre que se le da a cada división presente en una sola unidad física de almacenamiento de datos.

- **Directorio:** contenedor virtual en el que se almacenan una agrupación de archivos informáticos y otros subdirectorios, atendiendo a su contenido, a su propósito o a cualquier criterio que decida el usuario.
- **.doc, .jpg, .pdf…:** extensiones de un archivo, es decir el tipo de archivo y su formato (imagen, vídeo, documento de texto, archivo de audio, etc).
- **Línea de comandos:** es una interfaz de texto que nos permite interactuar con un proyecto, ejecutar tareas o navegar por todos los archivos y directorio de nuestro ordenador.

3.7. Análisis

El día 20 de marzo de 2023, a las 23:43, el perito D. Eduardo Villacampa Escartín recibe una llamada de la letrado Dª Noemi Ainsa Montañes, en nombre de D. Jorge Gutiérrez Palo. El motivo de la llamada es la contratación para realizar un peritaje sobre el ordenador de trabajo de su cliente, con el objetivo de certificar que se borró un archivo de su sistema.

El día 21 de marzo de 2023, a las 9:34, el perito D. Eduardo Villacampa Escartín acudió a las instalaciones de la empresa Microinformática Huesca S.L. con el objetivo de realizar un volcado de memoria y un clonado de disco del ordenador de D. Jorge Gutiérrez Palo.

Alrededor de las 12:50, el perito D. Eduardo Villacampa Escartín abandona las instalaciones de la empresa mencionada y acude lugar de trabajo del perito, localizado en Plaza Navarra, Nº.2, 2ª, 22002 (Huesca).

Sobre las 13:15 comienza el análisis de las evidencias recopiladas, con el objetivo de investigar si el archivo *"Redalyc_El_libro_digital_nuevos_formatos_de_lectura.pdf"* fue eliminado del ordenador de D. Jorge Gutiérrez Palo.

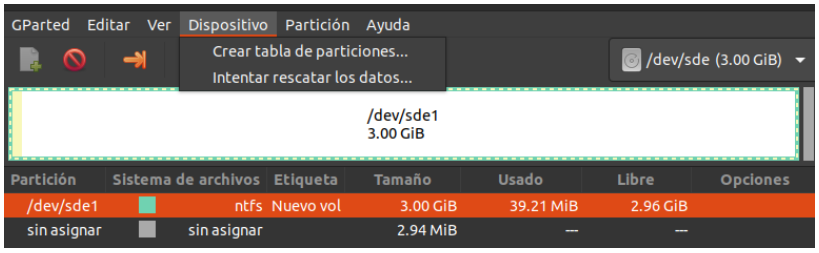
Para realizar el análisis, se han utilizado tres programas de recuperación de datos: Gparted, Foremost y Photorec.

Recuperación con Gparted

- Una vez instalado el programa, se debe elegir la partición concreta, en este caso, "sde1":

```
sde      8:64   0    3G  0 disk
└─sde1   8:65   0    3G  0 part
```

- Iniciar Gparted, seleccionar la partición deseada y pulsar la opción "intentar rescatar los datos" en "Dispositivos":



- A continuación, nos mostrará la información recuperada en caso de existir. Como se puede observar a continuación, no ha recuperado ningún archivo:

Recuperación con Foremost

- Creación del directorio en el que almacenaremos la información recuperada:

```
root@Estacion2EVillacampa:/home/usuario# mkdir eforemost
```

- Ejecución del programa sobre la partición deseada, mediante la línea de comandos:

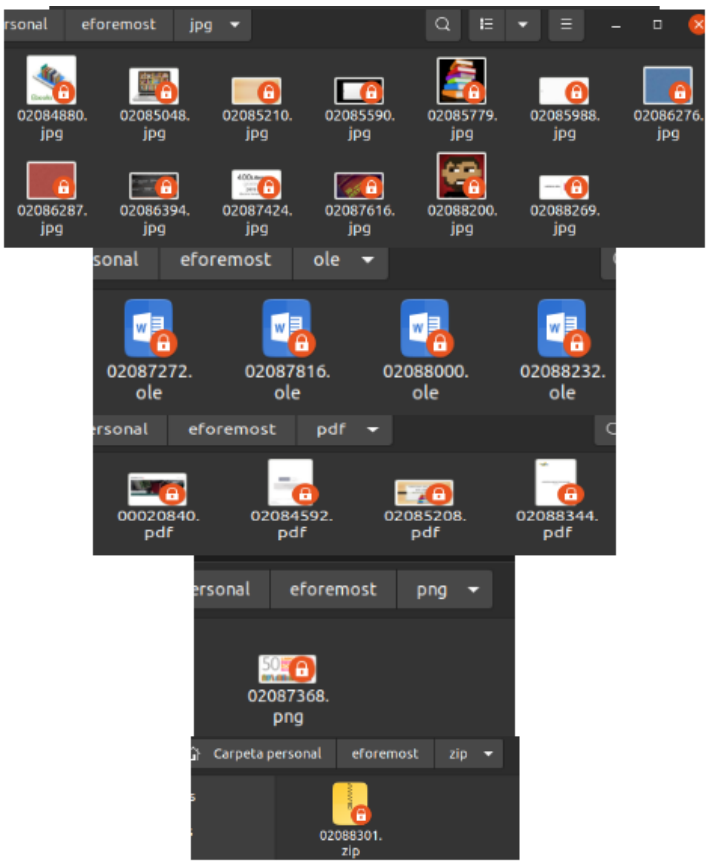
```
root@Estacion2EVillacampa:/home/usuario# foremost -v -i /dev/sde1 -o ./eforemost/
```

- A continuación, nos muestra el resumen de la información recuperada:

```
Finish: Thu Feb  2 18:01:32 2023

23 FILES EXTRACTED

jpg:= 13
ole:= 4
zip:= 1
png:= 1
pdf:= 4
----------------------------------------------------

Foremost finished at Thu Feb  2 18:01:32 2023
root@Estacion2EVillacampa:/home/usuario# fore
```

Podemos observar que ha recuperado imágenes, ficheros comprimidos y documentos.

- Accedemos al directorio que hemos elegido para guardar la información recuperada:



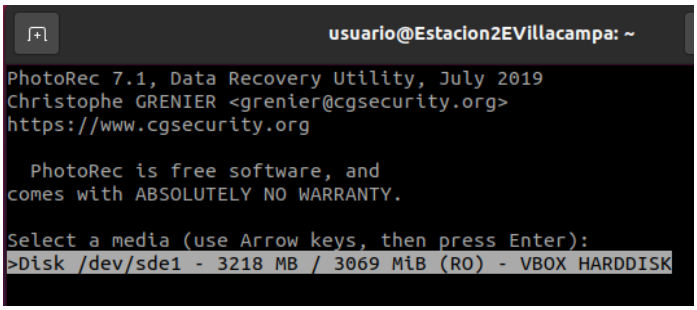
Recuperación con Photorec

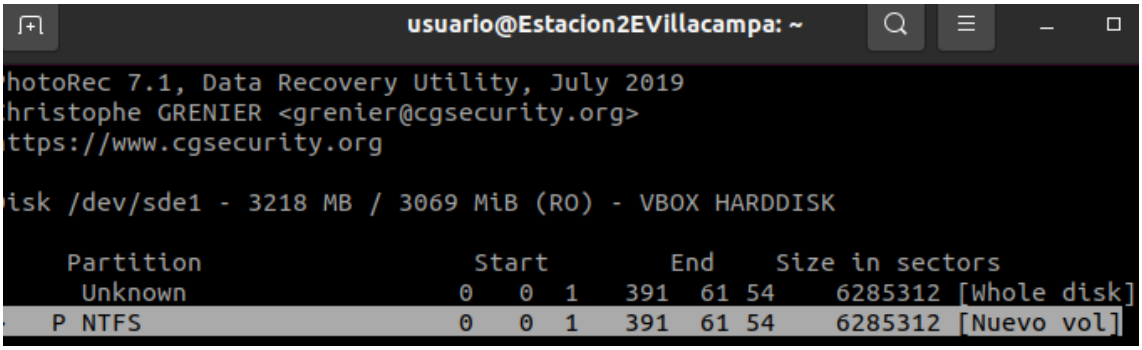
- Creación del directorio para almacenar la información recuperada:

```
root@Estacion2EVillacampa:/home/usuario# mkdir recovery
```

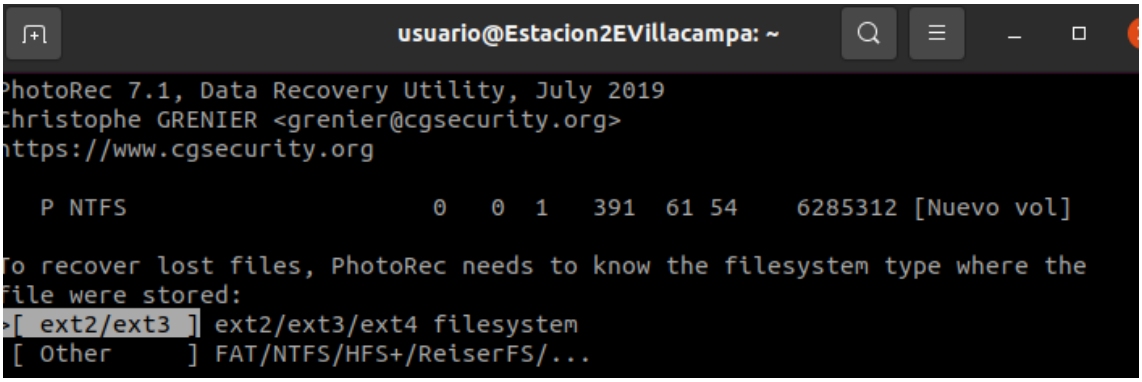
- Ejecutamos el programa sobre la partición deseada:

```
usuario@Estacion2EVillacampa:~$ sudo photorec /dev/sde1
```

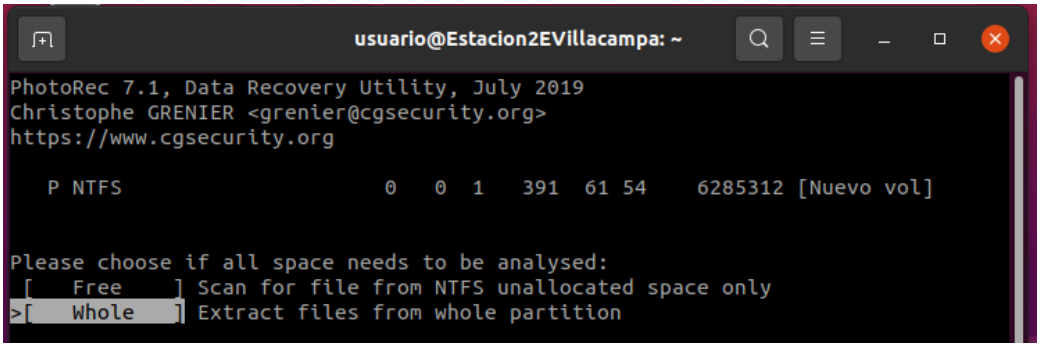




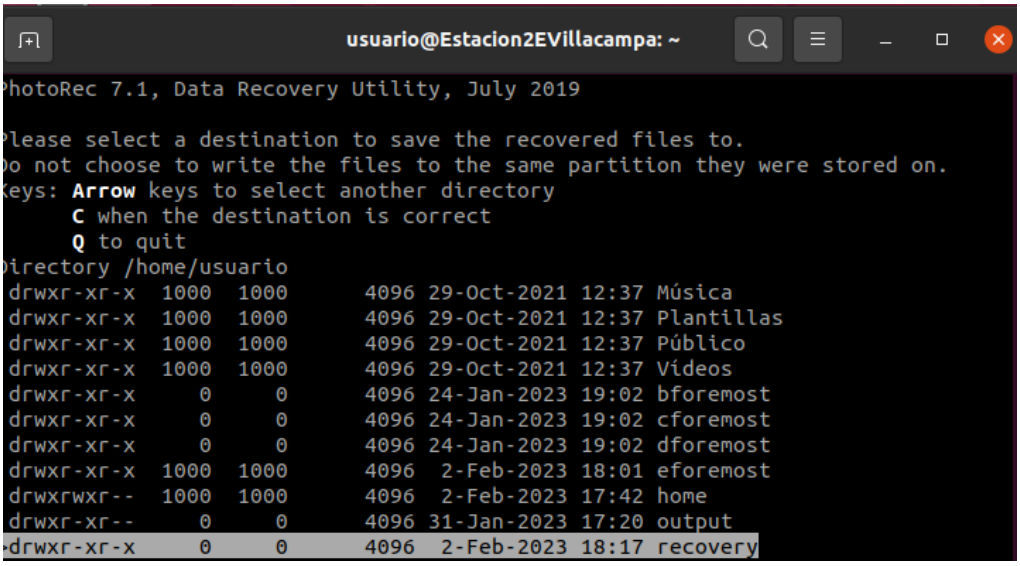
- Elegimos el sistema de ficheros de la partición:



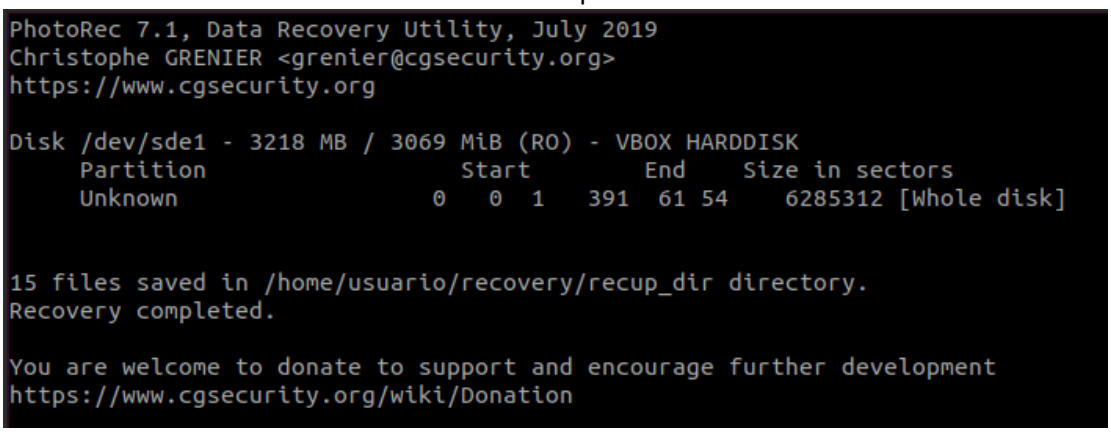
- Seleccionamos que extraiga los archivos de la partición completa:



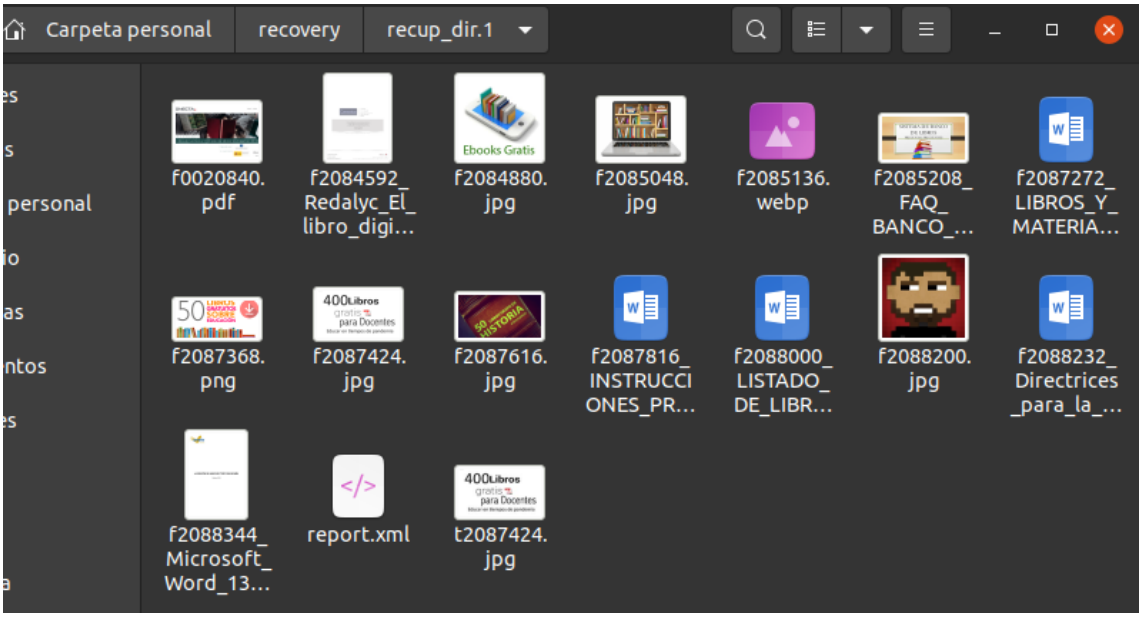
- Por último, seleccionamos el directorio donde almacenar la información recuperada, creado anteriormente:



- Nos muestra un resumen de la información recuperada:



- Accedemos al directorio que almacena la información:



-

-

3.8. Conclusiones

Una vez finalizado el análisis de las evidencias, podemos llegar a las siguientes conclusiones:

Listado de archivos recuperados

- **Archivos recuperados por Gparted:** ninguno.
- **Archivos recuperados por Foremost:** Total de 23 archivos recuperados.
  - **Archivos ".jpg":**
    - 02084880.jpg
    - 02085048.jpg
    - 02085210.jpg
    - 02085590.jpg
    - 02085779.jpg
    - 02085988.jpg
    - 02086276.jpg
    - 02086287.jpg
    - 02086394.jpg
    - 02087424.jpg
    - 02087616.jpg
    - 02088200.jpg
    - 02088269.jpg
  - **Archivos ".ole":**
    - 02087272.ole
    - 02087816.ole
    - 02088000.ole
    - 02088232.ole
  - **Archivos ".pdf":**
    - 00020840.pdf
    - 02084592.pdf
    - 02085208.pdf
    - 02088344.pdf
  - **Archivos "png":**
    - 02087368.png
  - **Archivos ".zip":**
    - 02088301.zip
- **Archivos recuperados con Photorec: total de 15 archivos:**
  - **Archivos ".pdf":**
    - f0020840.pdf
    - 2084592_Redalyc_El_libro_digital_nuevos_formatos_de_lectura.pdf
    - f2085208_FAQ_BANCO_DE_LIBROS.pdf
    - f2088344_Microsoft_Word_130711BCK_ANELE_Sector_de_Libros_de_Texto_2014.pdf
  - **Archivos ".jpg":**
    - f2084880.jpg
    - f2085048.jpg
    - f2087368.png
    - f2087424.jpg
    - f2087616.jpg
    - f2088200.jpg
    - t2087424.jpg
  - **Archivos ".doc":**
    - f2087272_LIBROS_Y_MATERIAL_ESCOLAR.doc

- f2087816_INSTRUCCIONES_PROGRAMA_DE_GRATUIDAD_DE_LIBROS_DE_TEXTO.doc
- 2088000_LISTADO_DE_LIBROS_RECOMENDADOS_PARA_TRABAJAR_IGUALDAD_DE_OPORTUNIDADES_ENTRE_NI_OS_Y_NI_AS_Y_CONVIVENCIA.doc
- f2088232_Directrices_para_la_asignaci_n_del_ISBN_a_los_libros_electr_nicos_y_aplicaciones.doc

¿El archivo *"Redalyc_El_libro_digital_nuevos_formatos_de_lectura.pdf"* fue eliminado del ordenador de D. Jorge Gutiérrez Palo*?*

Tras estudiar las evidencias recopiladas en el ordenador de D. Jorge Gutiérrez Palo, el programa Photorec recuperó el archivo ***"Redalyc_El_libro_digital_nuevos_formatos_de_lectura.pdf".***

¿Quién borró el archivo?

Mediante este análisis forense no se ha podido establecer quién borró el archivo.

¿Cuándo se borró el archivo?

Mediante este análisis forense no ha sido posible saber cuándo se borró el archivo.

¿El archivo fue borrado intencionadamente?

Mediante este análisis forense no se ha podido establecer si el archivo se eliminó intencionadamente.

¿Cómo es posible recuperar el archivo si se ha borrado?

Cuando se elimina un archivo de forma normal (papelera de reciclaje) se mantiene guardada una "huella" del mismo en el disco de almacenamiento del ordenador, aunque esta no sea visible.

Existen programas de recuperación de datos, como los utilizados en este informe, que permiten recuperar datos borrados.

Para constancia a los efectos oportunos, se emite el presente informe en la ciudad de Huesca, 30 de marzo de 2023.

D.Eduardo Villacampa Escartín

Nº de colegiado 27453

4. ANEXOS

I. Acuerdo de confidencialidad

Este acuerdo se celebra entre D. José Gutiérrez Palo y D. Eduardo Villacampa Escartín.

Se acuerda lo siguiente:

1. Ninguna de las dos partes podrá comunicar los resultados de la investigación a ninguna persona no involucrada en el mismo.
2. Ninguna de las dos partes podrá comunicar el proceso de investigación realizado a terceras personas.
3. El perito, D. Eduardo Villacampa Escartín, deberá eliminar cualquier dato obtenido durante el proceso de adquisición de evidencias, una vez el caso sea cerrado.
4. El perito D. Eduardo Villacampa Escartín, no podrá distribuir información obtenida durante el proceso de adquisición de evidencias.

Ambas partes se comprometen al cumplimiento del presente acuerdo

D. Eduardo Villacampa Escartín

D. José Gutiérrez Palo